# The Secrecy Capacity Region of the Gaussian MIMO Multi-Receiver Wiretap Channel*

Ersen Ekrem Sennur Ulukus

Department of Electrical and Computer Engineering

University of Maryland, College Park, MD 20742

*ersen@umd.edu* *ulukus@umd.edu*

March 18, 2009

**Abstract**

In this paper, we consider the Gaussian multiple-input multiple-output (MIMO) multi-receiver wiretap channel in which a transmitter wants to have confidential communication with an arbitrary number of users in the presence of an external eavesdropper. We derive the secrecy capacity region of this channel for the most general case. We first show that even for the single-input single-output (SISO) case, existing converse techniques for the Gaussian scalar broadcast channel cannot be extended to this secrecy context, to emphasize the need for a new proof technique. Our new proof technique makes use of the relationships between the minimum-mean-square-error and the mutual information, and equivalently, the relationships between the Fisher information and the differential entropy. Using the intuition gained from the converse proof of the SISO channel, we first prove the secrecy capacity region of the degraded MIMO channel, in which all receivers have the same number of antennas, and the noise covariance matrices can be arranged according to a positive semi-definite order. We then generalize this result to the aligned case, in which all receivers have the same number of antennas, however there is no order among the noise covariance matrices. We accomplish this task by using the channel enhancement technique. Finally, we find the secrecy capacity region of the general MIMO channel by using some limiting arguments on the secrecy capacity region of the aligned MIMO channel. We show that the capacity achieving coding scheme is a variant of dirty-paper coding with Gaussian signals.

*This work was supported by NSF Grants CCF 04-47613, CCF 05-14846, CNS 07-16311 and CCF 07-29127.

# 1 Introduction

Information theoretic secrecy was initiated by Wyner in his seminal work [1]. Wyner considered a degraded wiretap channel, where the eavesdropper gets a degraded version of the legitimate receiver's observation. For this degraded model, he found the capacity-equivocation rate region where the equivocation rate refers to the portion of the message rate that can be delivered to the legitimate receiver, while the eavesdropper is kept totally ignorant of this part. Later, Csiszar and Korner considered the general wiretap channel, where there is no presumed degradation order between the legitimate user and the eavesdropper [2]. They found the capacity-equivocation rate region of this general, *not necessarily degraded*, wiretap channel.

In recent years, information theoretic secrecy has gathered a renewed interest, where most of the attention has been devoted to the multiuser extensions of the wiretap channel, see for example [3–21]. One natural extension of the wiretap channel to the multiuser setting is the problem of *secure broadcasting*. In this case, there is one transmitter which wants to communicate with several legitimate users in the presence of an external eavesdropper. Hereafter, we call this channel model the *multi-receiver wiretap channel*. Finding the secrecy capacity region for the most general form of this channel model seems to be quite challenging, especially if one remembers that, even without the eavesdropper, we do not know the the capacity region for the underlying channel, which is a general broadcast channel with an arbitrary number of users. However, we know the capacity region for some special classes of broadcast channels, which suggests that we might be able to find the secrecy capacity region for some special classes of multi-receiver wiretap channels. This suggestion has been taken into consideration in [8–11]. In particular, in [9–11], the degraded multi-receiver wiretap channel is considered, where there is a certain degradation order among the legitimate users and the eavesdropper. The corresponding secrecy capacity region is derived for the two-user case in [9], and for an arbitrary number of users in [10, 11]. The importance of this class lies in the fact that the Gaussian scalar multi-receiver wiretap channel belongs to this class.

In this work, we start with the Gaussian scalar multi-receiver wiretap channel, and find its secrecy capacity region. Although, in the later parts of the paper, we provide the secrecy capacity region of the Gaussian multiple-input multiple-output (MIMO) multi-receiver wiretap channel which subsumes the scalar case, there are two reasons for the presentation of the scalar case separately. The first one is to show that, existing converse techniques for the Gaussian scalar broadcast channel, i.e., the converse proofs of Bergmans [22] and El Gamal [23], cannot be extended in a straightforward manner to provide a converse proof for the Gaussian scalar multi-receiver wiretap channel. We explicitly show that the main ingredient of these two converses in [22, 23], which is the entropy-power inequality [24, 25], is not sufficient to conclude a converse for the secrecy capacity region. The second reason for the separate presentation is to present the main ingredients of the technique that we will use to provide a converse proof for the general MIMO channel in an isolated manner

in a simpler context. We provide two converse proofs for the Gaussian scalar multi-receiver wiretap channel. The first one uses the connection between the minimum-mean-square-error (MMSE) and the mutual information along with the properties of the MMSE [26, 27]. In additive Gaussian channels, the Fisher information, another important quantity in estimation theory, and the MMSE have a complementary relationship in the sense that one of them determines the other one, and vice versa [28]. Thus, the converse proof relying on the MMSE has a counterpart which replaces the Fisher information with the MMSE in the corresponding converse proof. Hence, the second converse uses the connection between the Fisher information and the differential entropy via the de Bruin identity [24, 25] along with the properties of the Fisher information. This reveals that either the Fisher information matrix or the MMSE matrix should play an important role in the converse proof of the MIMO case.

Keeping this motivation in mind, we consider the Gaussian MIMO multi-receiver wiretap channel next. Instead of directly tackling the most general case in which each receiver has an arbitrary number of antennas and an arbitrary noise covariance matrix, we first consider two sub-classes of MIMO channels. In the first sub-class, all receivers have the same number of antennas and the noise covariance matrices exhibit a positive semi-definite order, which implies the degradedness of these channels. Hereafter, we call this channel model the *degraded Gaussian MIMO multi-receiver wiretap channel*. In the second sub-class, although all receivers still have the same number of antennas as in the degraded case, the noise covariance matrices do not have to satisfy any positive semi-definite order. Hereafter, we call this channel model the *aligned Gaussian MIMO multi-receiver wiretap channel*. Our approach will be to first find the secrecy capacity region of the degraded case, then to generalize this result to the aligned case by using the *channel enhancement* technique [29]. Once we obtain the secrecy capacity region of the aligned case, we use this result to find the secrecy capacity region of the most general case by some limiting arguments as in [29, 30]. Thus, the main contribution and the novelty of our work is the way we prove the secrecy capacity region of the degraded Gaussian MIMO multi-receiver wiretap channel, since the remaining steps from then on are mainly adaptations of the existing proof techniques [29,30] to an eavesdropper and/or multiuser setting.

At this point, to clarify our contributions, it might be useful to note the similarity of the proof steps that we follow with those in [29], where the capacity region of the Gaussian MIMO broadcast channel was established. In [29] also, the authors considered the degraded, the aligned and the general cases successively. Although, both [29] and this paper has these same proof steps, there are differences between how and why these steps are taken. In [29], the main difficulty in obtaining the capacity region of the Gaussian MIMO broadcast channel was to extend Bergmans' converse for the scalar case to the degraded vector channel. This difficulty was overcome in [29] by the invention of the *channel enhancement* technique. However, as discussed earlier, Bergmans' converse cannot be extended to our secrecy context,

even for the degraded scalar case. Thus, we need a new technique which we construct by using the Fisher information matrix and the generalized de Bruin identity [31]. After we obtain the secrecy capacity region of the degraded MIMO channel, we adapt the channel enhancement technique to our setting to find the secrecy capacity region of the aligned MIMO channel. The difference of the way channel enhancement is used here as compared to the one in [29] comes from the presence of an eavesdropper, and its difference from the one in [30] is due to the presence of many legitimate users. After we find the secrecy capacity region of the aligned MIMO channel, we use the limiting arguments that appeared in [29, 30] to prove the secrecy capacity region of the general MIMO channel.

The single user version of the Gaussian MIMO multi-receiver wiretap channel we study here, i.e., the Gaussian MIMO wiretap channel, was solved by [32, 33] for the general case and by [34] for the 2-2-1 case. Their common proof technique was to derive a Sato-type outer bound on the secrecy capacity, and then to tighten this outer bound by searching over all possible correlation structures among the noise vectors of the legitimate user and the eavesdropper. Later, [30] gave an alternative, simpler proof by using the channel enhancement technique.

# 2 Multi-Receiver Wiretap Channels

In this section, we first revisit the multi-receiver wiretap channel. The general multi-receiver wiretap channel consists of one transmitter with an input alphabet $\mathcal{X}$, $K$ legitimate receivers with output alphabets $\mathcal{Y}_k$, $k = 1, \ldots, K$, and an eavesdropper with output alphabet $\mathcal{Z}$. The transmitter sends a confidential message to each user, say $w_k \in \mathcal{W}_k$ to the $k$th user, and all messages are to be kept secret from the eavesdropper. The channel is memoryless with a transition probability $p(y_1, y_2, \ldots, y_K, z|x)$.

A $(2^{nR_1}, \ldots, 2^{nR_K}, n)$ code for this channel consists of $K$ message sets, $\mathcal{W}_k = \{1, \ldots, 2^{nR_k}\}$, $k = 1, \ldots, K$, an encoder $f : \mathcal{W}_1 \times \ldots \times \mathcal{W}_K \to \mathcal{X}^n$, $K$ decoders, one at each legitimate receiver, $g_k : \mathcal{Y}_k \to \mathcal{W}_k$, $k = 1, \ldots, K$. The probability of error is defined as $P_e^n = \max_{k=1,\ldots,K} \Pr\left[g_k(Y_k^n) \neq (W_k)\right]$. A rate tuple $(R_1, \ldots, R_K)$ is said to be achievable if there exists a code with $\lim_{n\to\infty} P_e^n = 0$ and

$$\lim_{n\to\infty} \frac{1}{n} H(\mathcal{S}(W)|Z^n) \geq \sum_{k\in\mathcal{S}(W)} R_k, \quad \forall\ \mathcal{S}(W) \tag{1}$$

where $\mathcal{S}(W)$ denotes any subset of $\{W_1, \ldots, W_K\}$. Hence, we consider only perfect secrecy rates. The secrecy capacity region is defined as the closure of all achievable rate tuples.

The degraded multi-receiver wiretap channel exhibits the following Markov chain

$$X \to Y_1 \to \ldots \to Y_K \to Z \tag{2}$$

whose capacity region was established in [10, 11] for an arbitrary number of users and in [9] for two users.

**Theorem 1** *The secrecy capacity region of the degraded multi-receiver wiretap channel is given by the union of the rate tuples* $(R_1, \ldots, R_K)$ *satisfying*[1]

$$R_k \leq I(U_k; Y_k | U_{k+1}, Z), \quad k = 1, \ldots, K \tag{3}$$

*where* $U_1 = X, U_{K+1} = \phi$*, and the union is over all probability distributions of the form*

$$p(u_K)p(u_{K-1}|u_K) \ldots p(u_2|u_3)p(x|u_2) \tag{4}$$

We remark here that since the channel is degraded, i.e., we have the Markov chain in (2), the capacity expressions in (3) are equivalent to

$$R_k \leq I(U_k; Y_k | U_{k+1}) - I(U_k; Z | U_{k+1}), \;\; k = 1, \ldots, K \tag{5}$$

We will use this equivalent expression frequently hereafter. For the case of two users and one eavesdropper, i.e., $K = 2$, the expressions in (5) reduce to:

$$R_1 \leq I(X; Y_1 | U_2) - I(X; Z | U_2) \tag{6}$$

$$R_2 \leq I(U_2; Y_2) - I(U_2; Z) \tag{7}$$

Finding the secrecy capacity region of the two-user degraded multi-receiver wiretap channel is tantamount to finding the optimal joint distributions of $(X, U_2)$ that trace the boundary of the secrecy capacity region given in (6)-(7). For the $K$-user degraded multi-receiver wiretap channel, we need to find the optimal joint distributions of $(X, U_2, \ldots, U_K)$ in the form given in (4) that trace the boundary of the region expressed in (3).

# 3 Gaussian MIMO Multi-receiver Wiretap Channel

## 3.1 Degraded Gaussian MIMO Multi-receiver Wiretap Channel

In this paper, we first consider the degraded Gaussian MIMO multi-receiver wiretap channel which is defined through

$$\mathbf{Y}_k = \mathbf{X} + \mathbf{N}_k, \quad k = 1, \ldots, K \tag{8}$$

$$\mathbf{Z} = \mathbf{X} + \mathbf{N}_Z \tag{9}$$

[1] Although in [10, 11], this secrecy capacity region is expressed in a different form, the equivalence of the two expressions can be shown.

where the channel input $\mathbf{X}$ is subject to a covariance constraint

$$E\left[\mathbf{X}\mathbf{X}^\top\right] \preceq \mathbf{S} \tag{10}$$

where $\mathbf{S} \succ 0$, and $\{\mathbf{N}_k\}_{k=1}^K, \mathbf{N}_Z$ are zero-mean Gaussian random vectors with covariance matrices $\{\boldsymbol{\Sigma}_k\}_{k=1}^K, \boldsymbol{\Sigma}_Z$ which satisfy the following ordering

$$\mathbf{0} \prec \boldsymbol{\Sigma}_1 \preceq \boldsymbol{\Sigma}_2 \preceq \ldots \preceq \boldsymbol{\Sigma}_K \preceq \boldsymbol{\Sigma}_Z \tag{11}$$

In a multi-receiver wiretap channel, since the capacity-equivocation rate region depends only on the conditional marginal distributions of the transmitter-receiver links, but not on the entire joint distribution of the channel, the correlations among $\{\mathbf{N}_k\}_{k=1}^K, \mathbf{N}_Z$ have no consequence on the capacity-equivocation rate region. Thus, without changing the corresponding secrecy capacity region, we can adjust the correlation structure among these noise vectors to ensure that they satisfy the following Markov chain

$$\mathbf{X} \to \mathbf{Y}_1 \to \ldots \to \mathbf{Y}_K \to \mathbf{Z} \tag{12}$$

which is always possible because of our assumption regarding the covariance matrices in (11). Moreover, the Markov chain in (12) implies that any Gaussian MIMO multi-receiver wiretap channel satisfying the semi-definite ordering in (11) can be treated as a degraded multi-receiver wiretap channel, hence Theorem 1 gives its capacity region. Hereafter, we will assume that the degraded Gaussian MIMO wiretap channel satisfies the Markov chain in (12).

## 3.2 Aligned Gaussian MIMO Multi-receiver Wiretap Channel

Next, we consider the aligned Gaussian MIMO multi-receiver wiretap channel which is again defined by (8)-(9), and the input is again subject to a covariance constraint as in (10) with $\mathbf{S} \succ \mathbf{0}$. However, for the aligned Gaussian MIMO multi-receiver wiretap channel, noise covariance matrices do not have any semi-definite ordering, as opposed to the degraded case which exhibits the ordering in (11). For the aligned Gaussian MIMO multi-receiver wiretap channel, the only assumption on the noise covariance matrices is that they are strictly positive-definite, i.e., $\boldsymbol{\Sigma}_i \succ \mathbf{0},\ i = 1, \ldots, K$ and $\boldsymbol{\Sigma}_Z \succ \mathbf{0}$. Since this channel does not have any ordering among the noise covariance matrices, it cannot be considered as a degraded channel, thus there is no single-letter formula for its secrecy capacity region. Moreover, we do not expect superposition coding with stochastic encoding to be optimal, as it was optimal for the degraded channel. Indeed, we will show that dirty-paper coding with stochastic encoding is optimal in this case.

### 3.3 General Gaussian MIMO Multi-receiver Wiretap Channel

Finally, we consider the most general form of the Gaussian MIMO multi-receiver wiretap channel which is given by

$$\mathbf{Y}_k = \mathbf{H}_k\mathbf{X} + \mathbf{N}_k, \quad k = 1, \ldots, K \tag{13}$$

$$\mathbf{Z} = \mathbf{H}_Z\mathbf{X} + \mathbf{N}_Z \tag{14}$$

where the channel input $\mathbf{X}$, which is a $t \times 1$ column vector, is again subject to a covariance constraint as in (10) with $\mathbf{S} \succeq \mathbf{0}$. The channel output for the $k$th user is denoted by $\mathbf{Y}_k$ which is a column vector of size $r_k \times 1$, $k = 1, \ldots, K$. The eavesdropper's observation $\mathbf{Z}$ is of size $r_Z \times 1$. The covariance matrices of the Gaussian random vectors $\{\mathbf{N}_k\}_{k=1}^K, \mathbf{N}_Z$ are denoted by $\{\mathbf{\Sigma}_k\}_{k=1}^K, \mathbf{\Sigma}_Z$, which are assumed to be strictly positive definite. The channel gain matrices $\{\mathbf{H}_k\}_{k=1}^K, \mathbf{H}_Z$ are of sizes $\{r_k \times t\}_{k=1}^K, r_Z \times t$, respectively, and they are known to the transmitter, all legitimate users and the eavesdropper.

### 3.4 A Comment on the Covariance Constraint

In the literature, it is more common to define capacity regions under a total power constraint, i.e., $\operatorname{tr}\left(E\left[\mathbf{X}\mathbf{X}^\top\right]\right) \leq P$, instead of the covariance constraint that we imposed, i.e., $E\left[\mathbf{X}\mathbf{X}^\top\right] \preceq \mathbf{S}$. However, as shown in [29], once the capacity region is obtained under a covariance constraint, then the capacity region under more lenient constraints on the channel inputs can be obtained, if these constraints can be expressed as compact sets defined over the input covariance matrices. For example, the total power constraint and the per-antenna power constraint can be described by compact sets of input covariance matrices as follows

$$\mathcal{S}^{\text{total}} = \{\mathbf{S} \succeq \mathbf{0} : \operatorname{tr}(\mathbf{S}) \leq P\} \tag{15}$$

$$\mathcal{S}^{\text{per}-\text{ant}} = \{\mathbf{S} \succeq \mathbf{0} : \mathbf{S}_{ii} \leq P_i, \ i = 1, \ldots, t\} \tag{16}$$

respectively, where $\mathbf{S}_{ii}$ is the $i$th diagonal entry of $\mathbf{S}$, and $t$ denotes the number of transmit antennas. Thus, if the secrecy capacity region under a covariance constraint $E\left[\mathbf{X}\mathbf{X}^\top\right] \preceq \mathbf{S}$ is found and denoted by $\mathcal{C}(\mathbf{S})$, then the secrecy capacity regions under the total power constraint and the per-antenna power constraint can be expressed as

$$\mathcal{C}^{\text{total}} = \bigcup_{\mathbf{S} \in \mathcal{S}^{\text{total}}} \mathcal{C}(\mathbf{S}) \tag{17}$$

$$\mathcal{C}^{\text{per}-\text{ant}} = \bigcup_{\mathbf{S} \in \mathcal{S}^{\text{per}-\text{ant}}} \mathcal{C}(\mathbf{S}) \tag{18}$$

respectively.

One other comment about the covariance constraint on the channel input is regarding the positive definiteness of $\mathbf{S}$. Following Lemma 2 of [29], it can be shown that, for any

degraded (resp. aligned) Gaussian MIMO multi-receiver channel under a covariance constraint $E\left[\mathbf{X}\mathbf{X}^\top\right] \preceq \mathbf{S}$ where $\mathbf{S}$ is a non-invertible positive semi-definite matrix, i.e., $\mathbf{S} \succeq \mathbf{0}$ and $|\mathbf{S}| = 0$, we can find another equivalent degraded (resp. aligned) channel with fewer transmit and receive antennas under a covariance constraint $E\big[\hat{\mathbf{X}}\hat{\mathbf{X}}^\top\big] \preceq \mathbf{S}'$ such that $\mathbf{S}' \succ \mathbf{0}$. Here the equivalence refers to the fact that both of these channels will have the same secrecy capacity region. Thus, as long as a degraded or an aligned channel is considered, there is no loss of generality in imposing a covariance constraint with a strictly positive definite matrix $\mathbf{S}$, and this is why we assumed that $\mathbf{S}$ is strictly positive definite for the degraded and the aligned channels.

# 4 Gaussian SISO Multi-receiver Wiretap Channel

We first visit the Gaussian SISO multi-receiver wiretap channel. The aims of this section are to show that a straightforward extension of existing converse techniques for the Gaussian scalar broadcast channel fails to provide a converse proof for the Gaussian SISO multi-receiver wiretap channel, and to provide an alternative proof technique using either the MMSE or the Fisher information along with their connections with the differential entropy. To this end, we first define the Gaussian SISO multi-receiver wiretap channel

$$Y_k = X + N_k, \quad k = 1, 2 \tag{19}$$

$$Z = X + N_Z \tag{20}$$

where we also restrict our attention to the two-user case for simplicity of the presentation. The channel input $X$ is subject to a power constraint $E\left[X^2\right] \leq P$. The variances of the zero-mean Gaussian random variables $N_1, N_2, N_Z$ are given by $\sigma_1^2, \sigma_2^2, \sigma_Z^2$, respectively, and satisfy the following order

$$\sigma_1^2 \leq \sigma_2^2 \leq \sigma_Z^2 \tag{21}$$

Since the correlations among $N_1, N_2, N_Z$ have no effect on the secrecy capacity region, we can adjust the correlation structure to ensure the following Markov chain

$$X \rightarrow Y_1 \rightarrow Y_2 \rightarrow Z \tag{22}$$

Thus, this channel can be considered as a degraded channel, and its secrecy capacity region is given by Theorem 1, in particular, by (6) and (7). Hence, to compute the secrecy capacity region explicitly, we need to find the optimal joint distributions of $(X, U_2)$ in (6) and (7). The corresponding secrecy capacity region is given by the following theorem.

**Theorem 2** *The secrecy capacity region of the two-user Gaussian SISO wiretap channel is*

*given by the union of the rate pairs* $(R_1, R_2)$ *satisfying*

$$R_1 \leq \frac{1}{2}\log\left(1+\frac{\alpha P}{\sigma_1^2}\right)-\frac{1}{2}\log\left(1+\frac{\alpha P}{\sigma_Z^2}\right) \tag{23}$$

$$R_2 \leq \frac{1}{2}\log\left(1+\frac{\bar{\alpha} P}{\alpha P+\sigma_2^2}\right)-\frac{1}{2}\log\left(1+\frac{\bar{\alpha} P}{\alpha P+\sigma_Z^2}\right) \tag{24}$$

*where the union is over all* $\alpha \in [0,1]$*, and* $\bar{\alpha}$ *denotes* $1-\alpha$*.*

The achievability of this region can be shown by selecting $(X, U_2)$ to be jointly Gaussian in Theorem 1. We focus on the converse proof.

## 4.1 Insufficiency of the Entropy-Power Inequality

As a natural approach, one might try to adopt the converse proofs of the scalar Gaussian broadcast channel for the converse proof of Theorem 2. In the literature, there are two converses for the Gaussian scalar broadcast channel which share some main principles. The first converse was given by Bergmans [22] who used Fano's lemma in conjunction with the entropy-power inequality [24,25] to find the capacity region. Later, El Gamal gave a relatively simple proof [23] which does not recourse to Fano's lemma. Rather, he started from the single-letter expression for the capacity region and used entropy-power inequality [24, 25] to evaluate this region. Thus, the entropy-power inequality [24, 25] is the main ingredient of these converses.

We now attempt to extend these converses to our secrecy context, i.e., to provide the converse proof of Theorem 2, and show where the argument breaks. In particular, what we will show in the following discussion is that a stand-alone use of the entropy-power inequality [24, 25] falls short of proving the optimality of Gaussian signalling in this secrecy context, as opposed to the Gaussian scalar broadcast channel. For that purpose, we consider El Gamal's converse for the Gaussian scalar broadcast channel. However, since the entropy-power inequality is in a central role for both El Gamal's and Bergmans' converse, the upcoming discussion can be carried out by using Bergmans' proof as well.

First, we consider the bound on the second user's secrecy rate. Using (7), we have

$$I(U_2;Y_2)-I(U_2;Z)=\big[I(X;Y_2)-I(X;Z)\big]-\big[I(X;Y_2|U_2)-I(X;Z|U_2)\big] \tag{25}$$

where the right-hand side is obtained by using the chain rule, and the Markov chain $U_2 \rightarrow X \rightarrow (Y_1, Y_2, Z)$. The expression in the first bracket is maximized by Gaussian $X$ [35] yielding

$$I(X;Y_2)-I(X;Z) \leq \frac{1}{2}\log\left(1+\frac{P}{\sigma_2^2}\right)-\frac{1}{2}\log\left(1+\frac{P}{\sigma_Z^2}\right) \tag{26}$$

Moreover, using the Markov chain $U_2 \rightarrow X \rightarrow Y_2 \rightarrow Z$, we can bound the expression in the

second bracket as

$$
\begin{aligned}
0 &\leq I(X;Y_2|U_2) - I(X;Z|U_2) && (27)\\
&\leq I(X;Y_2) - I(X;Z) && (28)\\
&\leq \frac{1}{2}\log\left(1+\frac{P}{\sigma_2^2}\right) - \frac{1}{2}\log\left(1+\frac{P}{\sigma_Z^2}\right) && (29)
\end{aligned}
$$

which implies that for any $(X, U_2)$ pair, there exists an $\alpha \in [0,1]$ such that

$$
I(X;Y_2|U_2) - I(X;Z|U_2) = \frac{1}{2}\log\left(1+\frac{\alpha P}{\sigma_2^2}\right) - \frac{1}{2}\log\left(1+\frac{\alpha P}{\sigma_Z^2}\right) \tag{30}
$$

Combining (26) and (30) in (25) yields the desired bound on $R_2$ given in (24).

From now on, we focus on obtaining the bound given in (23) on the first user's secrecy rate. To this end, one needs to solve the following optimization[2]

$$
\begin{aligned}
&\max \;\; I(X;Y_1|U_2) - I(X;Z|U_2) && (31)\\
&\text{s.t.} \quad I(X;Y_2|U_2) - I(X;Z|U_2) = \frac{1}{2}\log\left(1+\frac{\alpha P}{\sigma_2^2}\right) - \frac{1}{2}\log\left(1+\frac{\alpha P}{\sigma_Z^2}\right) && (32)
\end{aligned}
$$

When the term $I(X;Z|U_2)$ is absent in both the objective function and the constraint, as in the case of the Gaussian scalar broadcast channel, the entropy-power inequality [24, 25] can be used to solve this optimization problem. However, the presence of this term complicates the situation, and a stand-alone use of the entropy-power inequality [24, 25] does not seem to be sufficient. To substantiate this claim, let us consider the objective function in (31)

$$
\begin{aligned}
I(X;Y_1|U_2) - I(X;Z|U_2) &= h(Y_1|U_2) - h(Z|U_2) - \frac{1}{2}\log\frac{\sigma_1^2}{\sigma_Z^2} && (33)\\
&\leq \frac{1}{2}\log\left(e^{2h(Z|U_2)} - 2\pi e\left(\sigma_Z^2 - \sigma_1^2\right)\right) - h(Z|U_2) - \frac{1}{2}\log\frac{\sigma_1^2}{\sigma_Z^2} && (34)
\end{aligned}
$$

where the inequality is obtained by using the entropy-power inequality. Since the right-hand side of (34) is monotonically increasing in $h(Z|U_2)$, to show the optimality of Gaussian signalling, we need

$$
h(Z|U_2) \leq \frac{1}{2}\log 2\pi e(\alpha P + \sigma_Z^2) \tag{35}
$$

[2] Equivalently, one can consider the following optimization problem

$$
\begin{aligned}
&\max \;\; I(X;Y_1|U_2) - I(X;Y_2|U_2)\\
&\text{s.t.} \quad I(X;Y_2|U_2) - I(X;Z|U_2) = \frac{1}{2}\log\left(1+\frac{\alpha P}{\sigma_2^2}\right) - \frac{1}{2}\log\left(1+\frac{\alpha P}{\sigma_Z^2}\right)
\end{aligned}
$$

which, in turn, would yield a similar contradiction.

which will result in the desired bound on (31), i.e., the following

$$I(X;Y_1|U_2) - I(X;Z|U_2) \leq \frac{1}{2}\log\left(1+\frac{\alpha P}{\sigma_1^2}\right) - \frac{1}{2}\log\left(1+\frac{\alpha P}{\sigma_Z^2}\right) \tag{36}$$

which is the desired end-result in (23).

We now check whether (35) holds under the constraint given in (32). To this end, consider the difference of mutual informations in (32)

$$I(X;Y_2|U_2) - I(X;Z|U_2) = h(Y_2|U_2) - h(Z|U_2) - \frac{1}{2}\log\frac{\sigma_2^2}{\sigma_Z^2} \tag{37}$$

$$\leq \frac{1}{2}\log\left(e^{2h(Z|U_2)} - 2\pi e\left(\sigma_Z^2 - \sigma_2^2\right)\right) - h(Z|U_2) - \frac{1}{2}\log\frac{\sigma_2^2}{\sigma_Z^2} \tag{38}$$

where the inequality is obtained by using the entropy-power inequality. Now, using the constraint given in (32) in (38), we get

$$\frac{1}{2}\log\left(\frac{\alpha P+\sigma_2^2}{\alpha P+\sigma_Z^2}\right) \leq \frac{1}{2}\log\left(e^{2h(Z|U_2)} - 2\pi e\left(\sigma_Z^2 - \sigma_2^2\right)\right) - h(Z|U_2) \tag{39}$$

which implies

$$\frac{1}{2}\log 2\pi e(\alpha P+\sigma_Z^2) \leq h(Z|U_2) \tag{40}$$

Thus, as opposed to the inequality that we need to show the optimality of Gaussian signalling via the entropy-power inequality, i.e., the bound in (35), we have an opposite inequality. This discussion reveals that if Gaussian signalling is optimal, then its proof cannot be deduced from a straightforward extension of the converse proofs for the Gaussian scalar broadcast channel in [22, 23]. Thus, we need a new technique to provide the converse for Theorem 2. We now present two different proofs. The first proof relies on the relationship between the MMSE and the mutual information along with the properties of the MMSE, and the second proof replaces the MMSE with the Fisher information.

## 4.2 Converse for Theorem 2 Using the MMSE

We now provide a converse which uses the connection between the MMSE and the mutual information established in [26, 27]. In [27], the authors also give an alternative converse for the scalar Gaussian broadcast channel. Our proof will follow this converse, and generalize it to the context where there are secrecy constraints.

First, we briefly state the necessary background information. Let $N$ be a zero-mean unit-variance Gaussian random variable, and $(U, X)$ be a pair of arbitrarily correlated random variables which are independent of $N$. The MMSE of $X$ when it is observed through $U$ and

$\sqrt{t}X + N$ is

$$\mathrm{mmse}(X,t|U) = E\left[\left(X - E\left[X|\sqrt{t}X+N,U\right]\right)^2\right] \tag{41}$$

As shown in [26,27], the MMSE and the conditional mutual information are related through

$$I(X;\sqrt{t}X+N|U) = \frac{1}{2}\int_0^t \mathrm{mmse}(X,t|U)dt \tag{42}$$

For our converse, we need the following proposition which was proved in [27].

**Proposition 1 ([27],Proposition 12)** *Let $U, X, N$ be as specified above. The function*

$$f(t) = \frac{\sigma^2}{\sigma^2 t + 1} - \mathrm{mmse}(X,t|U) \tag{43}$$

*has at most one zero in $[0,\infty)$ unless $X$ is Gaussian conditioned on $U$ with variance $\sigma^2$, in which case the function is identically zero on $[0,\infty)$. In particular, if $t_0 < \infty$ is the unique zero, then $f(t)$ is strictly increasing on $[0,t_0]$, and strictly positive on $(t_0,\infty)$.*

We now give the converse. We use exactly the same steps from (25) to (30) to establish the bound on the secrecy rate of the second user given in (24). To bound the secrecy rate of the first user, we first restate (30) as

$$\begin{aligned} I(X;Y_2|U_2) - I(X;Z|U_2) &= I(X;(1/\sigma_2)X+N|U_2) - I(X;(1/\sigma_Z)X+N|U_2) && (44)\\ &= \frac{1}{2}\log\left(1+\frac{\alpha P}{\sigma_2^2}\right) - \frac{1}{2}\log\left(1+\frac{\alpha P}{\sigma_Z^2}\right) && (45)\\ &= \frac{1}{2}\int_{1/\sigma_Z^2}^{1/\sigma_2^2} \frac{\alpha P}{t\alpha P+1}dt && (46)\end{aligned}$$

Furthermore, due to (42), we also have

$$\begin{aligned} I(X;Y_2|U_2) - I(X;Z|U_2) &= I(X;(1/\sigma_2)X+N|U_2) - I(X;(1/\sigma_Z)X+N|U_2)\\ &= \frac{1}{2}\int_{1/\sigma_Z^2}^{1/\sigma_2^2} \mathrm{mmse}(X,t|U_2)dt && (47)\end{aligned}$$

Comparing (46) and (47) reveals that either we have

$$\mathrm{mmse}(X,t|U_2) = \frac{\alpha P}{t\alpha P+1} \tag{48}$$

for all $t \in [1/\sigma_Z^2, 1/\sigma_2^2]$, or there exists a unique $t_0 \in (1/\sigma_Z^2, 1/\sigma_2^2)$ such that

$$\mathrm{mmse}(X,t_0|U_2) = \frac{\alpha P}{t_0\alpha P+1} \tag{49}$$

and

$$\text{mmse}(X, t|U_2) \leq \frac{\alpha P}{t\alpha P + 1} \tag{50}$$

for $t > t_0$, because of Proposition 1. The former case occurs if $X$ is Gaussian conditioned on $U_2$ with variance $\alpha P$, in which case we arrive at the desired bound on the secrecy rate of the first user given in (23). If we assume that the latter case in (49)-(50) occurs, then, we can use the following sequence of derivations to bound the first user's secrecy rate

$$\begin{aligned}
I(X; Y_1|U_2) - I(X; Z|U_2) &= I(X; (1/\sqrt{\sigma_1})X + N|U_2) - I(X; (1/\sqrt{\sigma_Z})X + N|U_2) && (51)\\
&= \frac{1}{2}\int_{1/\sigma_Z^2}^{1/\sigma_1^2} \text{mmse}(X, t|U_2)dt && (52)\\
&= \frac{1}{2}\int_{1/\sigma_Z^2}^{1/\sigma_2^2} \text{mmse}(X, t|U_2)dt + \frac{1}{2}\int_{1/\sigma_2^2}^{1/\sigma_1^2} \text{mmse}(X, t|U_2)dt && (53)\\
&= \frac{1}{2}\log\left(1 + \frac{\alpha P}{\sigma_2^2}\right) - \frac{1}{2}\log\left(1 + \frac{\alpha P}{\sigma_Z^2}\right)\\
&\quad + \frac{1}{2}\int_{1/\sigma_2^2}^{1/\sigma_1^2} \text{mmse}(X, t|U_2)dt && (54)\\
&\leq \frac{1}{2}\log\left(1 + \frac{\alpha P}{\sigma_2^2}\right) - \frac{1}{2}\log\left(1 + \frac{\alpha P}{\sigma_Z^2}\right) + \frac{1}{2}\int_{1/\sigma_2^2}^{1/\sigma_1^2} \frac{\alpha P}{t\alpha P + 1}dt\\
& && (55)\\
&= \frac{1}{2}\log\left(1 + \frac{\alpha P}{\sigma_1^2}\right) - \frac{1}{2}\log\left(1 + \frac{\alpha P}{\sigma_Z^2}\right) && (56)
\end{aligned}$$

where (54) follows from (46) and (47), and (55) is due to (50). Since (56) is the desired bound on the secrecy rate of the first user given in (23), this completes the converse proof.

## 4.3 Converse for Theorem 2 Using the Fisher Information

We now provide an alternative converse which replaces the MMSE with the Fisher information in the above proof. We first provide some basic definitions. The unconditional versions of the following definition and the upcoming results regarding the Fisher information can be found in standard detection-estimation texts; to note one, [36] is a good reference for a detailed treatment of the subject.

**Definition 1** *Let $X, U$ be arbitrarily correlated random variables with well-defined densities, and $f(x|u)$ be the corresponding conditional density. The conditional Fisher information of*

*X is defined by*

$$J(X|U) = E\left[\left(\frac{\partial \log f(x|u)}{\partial x}\right)^2\right] \tag{57}$$

*where the expectation is over $(U, X)$.*

The vector generalization of the following conditional form of the Fisher information inequality will be given in Lemma 15 in Section 5.4, thus its proof is omitted here.

**Lemma 1** *Let $U, X, Y$ be random variables, and let the density for any combination of them exist. Moreover, let us assume that given $U$, $X$ and $Y$ are independent. Then, we have*

$$J(X+Y|U) \leq \beta^2 J(X|U) + (1-\beta)^2 J(Y|U) \tag{58}$$

*for any $\beta \in [0,1]$.*

**Corollary 1** *Let $X, Y, U$ be as specified above. Then, we have*

$$\frac{1}{J(X+Y|U)} \geq \frac{1}{J(X|U)} + \frac{1}{J(Y|U)} \tag{59}$$

**Proof:** Select

$$\beta = \frac{J(Y|U)}{J(X|U) + J(Y|U)} \tag{60}$$

in the previous lemma. ■

Similarly, the vector generalization of the following conditional form of the Cramer-Rao inequality will be given in Lemma 13 in Section 5.4, and hence, its proof is omitted here.

**Lemma 2** *Let $X, U$ be arbitrarily correlated random variables with well-defined densities. Then, we have*

$$J(X|U) \geq \frac{1}{\text{Var}(X|U)} \tag{61}$$

*with equality if $(U, X)$ is jointly Gaussian.*

We now provide the conditional form of the de Bruin identity [24, 25]. The vector generalization of this lemma will be provided in Lemma 16 in Section 5.4, and hence, its proof is omitted here.

**Lemma 3** *Let $X, U$ be arbitrarily correlated random variables with finite second order moments. Moreover, assume that they are independent of $N$ which is a zero-mean unit-variance*

*Gaussian random variable. Then, we have*

$$\frac{dh(X+\sqrt{t}N|U)}{dt} = \frac{1}{2}J(X+\sqrt{t}N|U) \tag{62}$$

We now note the following complementary relationship between the MMSE and the Fisher information [26, 28]

$$J(\sqrt{t}X+N) = 1 - t\cdot \mathrm{mmse}(X,t) \tag{63}$$

which itself suggests the existence of an alternative converse which uses the Fisher information instead of the MMSE. We now provide the alternative converse based on the Fisher information. We first bound the secrecy rate of the second user as in the previous section, by following the exact steps from (25) to (30). To bound the secrecy rate of the first user, we first rewrite (30) as follows

$$\begin{aligned} I(X;Y_2|U_2) - I(X;Z|U_2) &= h(X+\sigma_2 N|U_2) - h(X+\sigma_Z N|U_2) - \frac{1}{2}\log\frac{\sigma_2^2}{\sigma_Z^2} && (64)\\ &= -\frac{1}{2}\int_{\sigma_2^2}^{\sigma_Z^2} J(X+\sqrt{t}N|U_2)dt - \frac{1}{2}\log\frac{\sigma_2^2}{\sigma_Z^2} && (65)\\ &= -\frac{1}{2}\int_{\sigma_2^2}^{\sigma_Z^2} J(X+\sqrt{t-t^*}N'+\sqrt{t^*}N''|U_2)dt - \frac{1}{2}\log\frac{\sigma_2^2}{\sigma_Z^2} && (66) \end{aligned}$$

where (65) follows from Lemma 3, and in (66), we used the stability of Gaussian random variables where, $N', N''$ are two independent zero-mean unit-variance Gaussian random variables. Moreover, $t^*$ is selected in the range of $(0, \sigma_2^2)$. We now use Corollary 1 to bound the conditional Fisher information in (66) as follows

$$\begin{aligned} \frac{1}{J(X+\sqrt{t-t^*}N'+\sqrt{t^*}N''|U_2)} &\geq \frac{1}{J(X+\sqrt{t^*}N''|U_2)} + \frac{1}{J(\sqrt{t-t^*}N'|U_2)} && (67)\\ &= \frac{1}{J(X+\sqrt{t^*}N''|U_2)} + (t-t^*) && (68) \end{aligned}$$

where the equality follows from Lemma 2. The inequality in (68) is equivalent to

$$J(X+\sqrt{t-t^*}N'+\sqrt{t^*}N''|U_2) \leq \frac{J(X+\sqrt{t^*}N''|U_2)}{1+J(X+\sqrt{t^*}N''|U_2)(t-t^*)} \tag{69}$$

using which in (66) yields

$$I(X;Y_2|U_2) - I(X;Z|U_2) \geq -\frac{1}{2}\int_{\sigma_2^2}^{\sigma_Z^2} \frac{J(X+\sqrt{t^*}N''|U_2)}{1+J(X+\sqrt{t^*}N''|U_2)(t-t^*)}dt - \frac{1}{2}\log\frac{\sigma_2^2}{\sigma_Z^2} \tag{70}$$

$$= -\frac{1}{2}\log\frac{1+J(X+\sqrt{t^*}N''|U_2)(\sigma_Z^2-t^*)}{1+J(X+\sqrt{t^*}N''|U_2)(\sigma_2^2-t^*)} - \frac{1}{2}\log\frac{\sigma_2^2}{\sigma_Z^2} \tag{71}$$

We remind that we had already fixed the left-hand side of this inequality as

$$I(X;Y_2|U_2) - I(X;Z|U_2) = \frac{1}{2}\log\left(1+\frac{\alpha P}{\sigma_2^2}\right) - \frac{1}{2}\log\left(1+\frac{\alpha P}{\sigma_Z^2}\right) \tag{72}$$

in (30). Comparison of (71) and (72) results in

$$J(X+\sqrt{t^*}N''|U_2) \geq \frac{1}{\alpha P + t^*}, \quad 0 < t^* \leq \sigma_2^2 \tag{73}$$

At this point, we compare the inequalities in (50) and (73). These two inequalities imply each other through the complementary relationship between the MMSE and the Fisher information given in (63) after appropriate change of variables and by noting that $J(aX) = (1/a^2)J(X)$ [36]. We now find the desired bound on the secrecy rate of the first user via using the inequality in (73)

$$I(X;Y_1|U_2) - I(X;Z|U_2) = h(X+\sigma_1 N|U_2) - h(X+\sigma_Z N|U_2) - \frac{1}{2}\log\frac{\sigma_1^2}{\sigma_Z^2} \tag{74}$$

$$= -\frac{1}{2}\int_{\sigma_1^2}^{\sigma_Z^2} J(X+\sqrt{t}N|U_2)dt - \frac{1}{2}\log\frac{\sigma_1^2}{\sigma_Z^2} \tag{75}$$

$$= -\frac{1}{2}\int_{\sigma_1^2}^{\sigma_2^2} J(X+\sqrt{t}N|U_2)dt - \frac{1}{2}\int_{\sigma_2^2}^{\sigma_Z^2} J(X+\sqrt{t}N|U_2)dt - \frac{1}{2}\log\frac{\sigma_1^2}{\sigma_Z^2} \tag{76}$$

$$= -\frac{1}{2}\int_{\sigma_1^2}^{\sigma_2^2} J(X+\sqrt{t}N|U_2)dt - \frac{1}{2}\log\left(\frac{\alpha P+\sigma_Z^2}{\alpha P+\sigma_2^2}\right) - \frac{1}{2}\log\frac{\sigma_1^2}{\sigma_Z^2} \tag{77}$$

$$\leq -\frac{1}{2}\int_{\sigma_1^2}^{\sigma_2^2} \frac{1}{\alpha P+t}dt - \frac{1}{2}\log\left(\frac{\alpha P+\sigma_Z^2}{\alpha P+\sigma_2^2}\right) - \frac{1}{2}\log\frac{\sigma_1^2}{\sigma_Z^2} \tag{78}$$

$$= -\frac{1}{2}\log\left(\frac{\alpha P+\sigma_2^2}{\alpha P+\sigma_1^2}\right) - \frac{1}{2}\log\left(\frac{\alpha P+\sigma_Z^2}{\alpha P+\sigma_2^2}\right) - \frac{1}{2}\log\frac{\sigma_1^2}{\sigma_Z^2} \tag{79}$$

$$= \frac{1}{2}\log\left(1+\frac{\alpha P}{\sigma_1^2}\right) - \frac{1}{2}\log\left(1+\frac{\alpha P}{\sigma_Z^2}\right) \tag{80}$$

where (77) follows from (65) and (72), and (78) is due to (73). Since (80) provides the desired bound on the secrecy rate of the first user given in (23), this completes the converse proof.

### 4.4 Summary of the SISO Case, Outlook for the MIMO Case

In this section, we first revisited the standard converse proofs [22, 23] of the Gaussian scalar broadcast channel, and showed that a straightforward extension of these proofs will not be able to provide a converse proof for the Gaussian SISO multi-receiver wiretap channel. Basically, a stand-alone use of the entropy-power inequality [24, 25] falls short of resolving the ambiguity on the auxiliary random variables. We showed that, in this secrecy context, either the connection between the mutual information and the MMSE or the connection between the differential entropy and the Fisher information can be used, along with their properties, to come up with a converse.

In the next section, we will generalize this converse proof technique to the degraded MIMO channel. One way of generalizing this converse technique to the MIMO case might be to use the channel enhancement technique, which was successfully used in extending Bergmans' converse proof from the scalar Gaussian broadcast channel to the degraded vector Gaussian broadcast channel. We note that such an extension will not work in this secrecy context. In the degraded Gaussian MIMO broadcast channel, the non-trivial part of the converse proof was to extend Bergmans' converse to a vector case, and this was accomplished by the invention of the channel enhancement technique. However, as we have shown in Section 4.1, even in the Gaussian SISO multi-receiver wiretap channel, a Bergmans type converse does not work. Therefore, we will not pursue a channel enhancement approach to extend our proof from the SISO channel to the degraded MIMO channel. Instead, we will use the connections between the Fisher information and the differential entropy, as we did in Section 4.3, to come up with a converse proof for the degraded MIMO channel. We will then use the channel enhancement technique to extend our converse proof to the aligned MIMO channel. Finally, we will use some limiting arguments, as in [29, 30], to come up with a converse proof for the most general MIMO channel.

## 5 Degraded Gaussian MIMO Multi-receiver Wiretap Channel

In this section, we establish the secrecy capacity region of the degraded Gaussian MIMO multi-receiver wiretap channel. We state the main result of this section in the following theorem.

**Theorem 3** *The secrecy capacity region of the degraded Gaussian MIMO multi-receiver*

*wiretap channel is given by the union of the rate tuples $R_1, \ldots, R_K$ satisfying*

$$R_k \leq \frac{1}{2} \log \frac{\left|\sum_{i=1}^{k} \mathbf{K}_i + \mathbf{\Sigma}_k\right|}{\left|\sum_{i=1}^{k-1} \mathbf{K}_i + \mathbf{\Sigma}_k\right|} - \frac{1}{2} \log \frac{\left|\sum_{i=1}^{k} \mathbf{K}_i + \mathbf{\Sigma}_Z\right|}{\left|\sum_{i=1}^{k-1} \mathbf{K}_i + \mathbf{\Sigma}_Z\right|}, \quad k = 1, \ldots, K \tag{81}$$

*where the union is over all positive semi-definite matrices $\{\mathbf{K}_i\}_{i=1}^{K}$ that satisfy*

$$\sum_{i=1}^{K} \mathbf{K}_i = \mathbf{S} \tag{82}$$

The achievability of these rates follows from Theorem 1 by selecting $(U_K, \ldots, U_2, \mathbf{X})$ to be jointly Gaussian. Thus, to prove the theorem, we only need to provide a converse. Since the converse proof is rather long and involves technical digressions, we first present the converse proof for $K = 2$. In this process, we will develop all necessary tools which we will use to provide the converse proof for arbitrary $K$ in Section 5.5.

The secrecy capacity region of the two-user degraded MIMO channel, from (81), is the union of the rate pairs $(R_1, R_2)$ satisfying

$$R_1 \leq \frac{1}{2} \log \frac{|\mathbf{K}_1 + \mathbf{\Sigma}_1|}{|\mathbf{\Sigma}_1|} - \frac{1}{2} \log \frac{|\mathbf{K}_1 + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{83}$$

$$R_2 \leq \frac{1}{2} \log \frac{|\mathbf{S} + \mathbf{\Sigma}_2|}{|\mathbf{K}_1 + \mathbf{\Sigma}_2|} - \frac{1}{2} \log \frac{|\mathbf{S} + \mathbf{\Sigma}_Z|}{|\mathbf{K}_1 + \mathbf{\Sigma}_Z|} \tag{84}$$

where the union is over all selections of $\mathbf{K}_1$ that satisfies $\mathbf{0} \preceq \mathbf{K}_1 \preceq \mathbf{S}$. We note that these rates are achievable by choosing $\mathbf{X} = \mathbf{U}_2 + \mathbf{V}$ in Theorem 1, where $\mathbf{U}_2$ and $\mathbf{V}$ are independent Gaussian random vectors with covariance matrices $\mathbf{S} - \mathbf{K}_1$ and $\mathbf{K}_1$, respectively. Next, we prove that the union of the rate pairs in (83) and (84) constitute the secrecy capacity region of the two-user degraded MIMO channel.

## 5.1 Proof of Theorem 3 for $K = 2$

To prove that (83) and (84) give the secrecy capacity region, we need the results of some intermediate optimization problems. The first one is the so-called worst additive noise lemma [37, 38].

**Lemma 4** *Let $\mathbf{N}$ be a Gaussian random vector with covariance matrix $\mathbf{\Sigma}$, and $\mathbf{K}_X$ be a positive semi-definite matrix. Consider the following optimization problem,*

$$\begin{aligned} \min_{p(\mathbf{x})} \quad & I(\mathbf{N}; \mathbf{N} + \mathbf{X}) \\ \text{s.t.} \quad & \text{Cov}(\mathbf{X}) = \mathbf{K}_X \end{aligned} \tag{85}$$

*where* $\mathbf{X}$ *and* $\mathbf{N}$ *are independent. A Gaussian* $\mathbf{X}$ *is the minimizer of this optimization problem.*

The second optimization problem that will be useful in the upcoming proof is the conditional version of the following theorem.

**Theorem 4** *Let* $\mathbf{X}, \mathbf{N}_1, \mathbf{N}_2, \mathbf{N}_Z$ *be independent random vectors, where* $\mathbf{N}_1, \mathbf{N}_2, \mathbf{N}_Z$ *are zero-mean Gaussian random vectors with covariance matrices* $\mathbf{0} \prec \mathbf{\Sigma}_1 \preceq \mathbf{\Sigma}_2 \preceq \mathbf{\Sigma}_Z$*, respectively. Moreover, assume that the second moment of* $\mathbf{X}$ *is constrained as*

$$E\left[\mathbf{X}\mathbf{X}^\top\right] \preceq \mathbf{S} \tag{86}$$

*where* $\mathbf{S}$ *is a positive definite matrix. Then, for any admissible* $\mathbf{X}$*, there exists a matrix* $\mathbf{K}^*$ *such that* $\mathbf{0} \preceq \mathbf{K}^* \preceq \mathbf{S}$*, and*

$$h(\mathbf{X}+\mathbf{N}_Z) - h(\mathbf{X}+\mathbf{N}_2) = \frac{1}{2}\log\frac{|\mathbf{K}^*+\mathbf{\Sigma}_Z|}{|\mathbf{K}^*+\mathbf{\Sigma}_2|} \tag{87}$$

$$h(\mathbf{X}+\mathbf{N}_Z) - h(\mathbf{X}+\mathbf{N}_1) \geq \frac{1}{2}\log\frac{|\mathbf{K}^*+\mathbf{\Sigma}_Z|}{|\mathbf{K}^*+\mathbf{\Sigma}_1|} \tag{88}$$

The conditional version of Theorem 4 is given as follows.

**Theorem 5** *Let* $\mathbf{U}, \mathbf{X}$ *be arbitrarily correlated random vectors which are independent of* $\mathbf{N}_1, \mathbf{N}_2, \mathbf{N}_Z$*, where* $\mathbf{N}_1, \mathbf{N}_2, \mathbf{N}_Z$ *are zero-mean Gaussian random vectors with covariance matrices* $\mathbf{0} \prec \mathbf{\Sigma}_1 \preceq \mathbf{\Sigma}_2 \preceq \mathbf{\Sigma}_Z$*, respectively. Moreover, assume that the second moment of* $\mathbf{X}$ *is constrained as*

$$E\left[\mathbf{X}\mathbf{X}^\top\right] \preceq \mathbf{S} \tag{89}$$

*where* $\mathbf{S}$ *is a positive definite matrix. Then, for any admissible* $(\mathbf{U}, \mathbf{X})$ *pair, there exists a matrix* $\mathbf{K}^*$ *such that* $\mathbf{0} \preceq \mathbf{K}^* \preceq \mathbf{S}$*, and*

$$h(\mathbf{X}+\mathbf{N}_Z|\mathbf{U}) - h(\mathbf{X}+\mathbf{N}_2|\mathbf{U}) = \frac{1}{2}\log\frac{|\mathbf{K}^*+\mathbf{\Sigma}_Z|}{|\mathbf{K}^*+\mathbf{\Sigma}_2|} \tag{90}$$

$$h(\mathbf{X}+\mathbf{N}_Z|\mathbf{U}) - h(\mathbf{X}+\mathbf{N}_1|\mathbf{U}) \geq \frac{1}{2}\log\frac{|\mathbf{K}^*+\mathbf{\Sigma}_Z|}{|\mathbf{K}^*+\mathbf{\Sigma}_1|} \tag{91}$$

Theorem 4 serves as a step towards the proof of Theorem 5. Proofs of these two theorems are deferred to Sections 5.3 and 5.4.

We are now ready to show that the secrecy capacity region of the two-user degraded MIMO channel is given by (83)-(84). We first consider $R_2$, and bound it using Theorem 1

as follows

$$R_2 \leq I(U_2;\mathbf{Y}_2) - I(U_2;\mathbf{Z}) \tag{92}$$

$$= [I(\mathbf{X};\mathbf{Y}_2) - I(\mathbf{X};\mathbf{Z})] - [I(\mathbf{X};\mathbf{Y}_2|U_2) - I(\mathbf{X};\mathbf{Z}|U_2)] \tag{93}$$

where the equality is obtained by using the chain rule and the Markov chain $U_2 \rightarrow \mathbf{X} \rightarrow (\mathbf{Y}_2, \mathbf{Z})$. We now consider the expression in the first bracket of (93)

$$I(\mathbf{X};\mathbf{Y}_2) - I(\mathbf{X};\mathbf{Z}) = h(\mathbf{Y}_2) - h(\mathbf{Y}_2|\mathbf{X}) - h(\mathbf{Z}) + h(\mathbf{Z}|\mathbf{X}) \tag{94}$$

$$= h(\mathbf{Y}_2) - h(\mathbf{Z}) - \frac{1}{2}\log\frac{|\boldsymbol{\Sigma}_2|}{|\boldsymbol{\Sigma}_Z|} \tag{95}$$

where the second equality follows from the facts that $h(\mathbf{Y}_2|\mathbf{X}) = h(\mathbf{N}_2)$ and $h(\mathbf{Z}|\mathbf{X}) = h(\mathbf{N}_Z)$. We now consider the difference of differential entropies in (95). To this end, consider the Gaussian random vector $\tilde{\mathbf{N}}_2$ with covariance matrix $\boldsymbol{\Sigma}_Z - \boldsymbol{\Sigma}_2$, which is chosen to be independent of $\mathbf{X}, \mathbf{N}_2$. Using the Markov chain in (12), we get

$$h(\mathbf{Y}_2) - h(\mathbf{Z}) = h(\mathbf{Y}_2) - h(\mathbf{Y}_2 + \tilde{\mathbf{N}}_2) \tag{96}$$

$$= -I(\tilde{\mathbf{N}}_2;\mathbf{Y}_2 + \tilde{\mathbf{N}}_2) \tag{97}$$

$$\leq \max_{\mathbf{0}\preceq\mathbf{K}\preceq\mathbf{S}} \frac{1}{2}\log\frac{|\mathbf{K}+\boldsymbol{\Sigma}_2|}{|\mathbf{K}+\boldsymbol{\Sigma}_Z|} \tag{98}$$

$$= \frac{1}{2}\log\frac{|\mathbf{S}+\boldsymbol{\Sigma}_2|}{|\mathbf{S}+\boldsymbol{\Sigma}_Z|} \tag{99}$$

where (98) follows from Lemma 4 and (99) is a consequence of the fact that

$$\frac{|\mathbf{B}|}{|\mathbf{A}+\mathbf{B}|} \leq \frac{|\mathbf{B}+\boldsymbol{\Delta}|}{|\mathbf{A}+\mathbf{B}+\boldsymbol{\Delta}|} \tag{100}$$

when $\mathbf{A}, \mathbf{B}, \boldsymbol{\Delta} \succeq 0$, and $\mathbf{A}+\mathbf{B} \succ 0$ [29]. Plugging (99) into (95) yields

$$I(\mathbf{X};\mathbf{Y}_2) - I(\mathbf{X};\mathbf{Z}) \leq \frac{1}{2}\log\frac{|\mathbf{S}+\boldsymbol{\Sigma}_2|}{|\boldsymbol{\Sigma}_2|} - \frac{1}{2}\log\frac{|\mathbf{S}+\boldsymbol{\Sigma}_Z|}{|\boldsymbol{\Sigma}_Z|} \tag{101}$$

We now consider the expression in the second bracket of (93). For that purpose, we use Theorem 5. According to Theorem 5, for any admissible pair $(U_2, \mathbf{X})$, there exists a $\mathbf{K}^*$ such that

$$h(\mathbf{X}+\mathbf{N}_Z|U_2) - h(\mathbf{X}+\mathbf{N}_2|U_2) = \frac{1}{2}\log\frac{|\mathbf{K}^*+\boldsymbol{\Sigma}_Z|}{|\mathbf{K}^*+\boldsymbol{\Sigma}_2|} \tag{102}$$

which is equivalent to

$$I(\mathbf{X};\mathbf{Z}|U_2) - I(\mathbf{X};\mathbf{Y}_2|U_2) = \frac{1}{2}\log\frac{|\mathbf{K}^* + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} - \frac{1}{2}\log\frac{|\mathbf{K}^* + \mathbf{\Sigma}_2|}{|\mathbf{\Sigma}_2|} \tag{103}$$

Thus, using (101) and (103) in (93), we get

$$R_2 \le \frac{1}{2}\log\frac{|\mathbf{S} + \mathbf{\Sigma}_2|}{|\mathbf{K}^* + \mathbf{\Sigma}_2|} - \frac{|\mathbf{S} + \mathbf{\Sigma}_Z|}{|\mathbf{K}^* + \mathbf{\Sigma}_Z|} \tag{104}$$

which is the desired bound on $R_2$ given in (84). We now obtain the desired bound on $R_1$ given in (83). To this end, we first bound $R_1$ using Theorem 1

$$\begin{aligned} R_1 &\le I(\mathbf{X};\mathbf{Y}_1|U_2) - I(\mathbf{X};\mathbf{Z}|U_2) && (105)\\ &= h(\mathbf{Y}_1|U_2) - h(\mathbf{Y}_1|U_2,\mathbf{X}) - h(\mathbf{Z}|U_2) + h(\mathbf{Z}|U_2,\mathbf{X}) && (106)\\ &= h(\mathbf{Y}_1|U_2) - h(\mathbf{Z}|U_2) - \frac{1}{2}\log\frac{|\mathbf{\Sigma}_1|}{|\mathbf{\Sigma}_Z|} && (107)\end{aligned}$$

where the second equality follows from the facts that $h(\mathbf{Y}_1|U_2,\mathbf{X}) = h(\mathbf{N}_1)$ and $h(\mathbf{Z}|U_2,\mathbf{X}) = h(\mathbf{N}_Z)$. To bound the difference of conditional differential entropies in (107), we use Theorem 5. Theorem 5 states that for any admissible pair $(U_2,\mathbf{X})$, there exists a matrix $\mathbf{K}^*$ such that it satisfies (102) and also

$$h(\mathbf{Z}|U_2) - h(\mathbf{Y}_1|U_2) \ge \frac{1}{2}\log\frac{|\mathbf{K}^* + \mathbf{\Sigma}_Z|}{|\mathbf{K}^* + \mathbf{\Sigma}_1|} \tag{108}$$

Thus, using (108) in (107), we get

$$R_1 \le \frac{1}{2}\log\frac{|\mathbf{K}^* + \mathbf{\Sigma}_1|}{|\mathbf{\Sigma}_1|} - \frac{1}{2}\log\frac{|\mathbf{K}^* + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{109}$$

which is the desired bound on $R_1$ given in (83), completing the converse proof for $K = 2$.

As we have seen, the main ingredient in the above proof was Theorem 5. Therefore, to complete the converse proof for the degraded channel for $K = 2$, from this point on, we will focus on the proof of Theorem 5. We will give the proof of Theorem 5 in Section 5.4. In preparation to that, we will give the proof of Theorem 4, which is the unconditional version of Theorem 5, in Section 5.3. The proof of Theorem 4 involves the use of properties of the Fisher information, and its connection to the differential entropy, which are provided next.

## 5.2 The Fisher Information Matrix

We start with the definition [36].

**Definition 2** *Let* $\mathbf{U}$ *be a length-n random vector with differentiable density* $f_U(\mathbf{u})$*. The*

*Fisher information matrix of* $\mathbf{U}$, $\mathbf{J}(\mathbf{U})$, *is defined as*

$$\mathbf{J}(\mathbf{U}) = E\left[\boldsymbol{\rho}(\mathbf{U})\boldsymbol{\rho}(\mathbf{U})^\top\right] \tag{110}$$

*where* $\boldsymbol{\rho}(\mathbf{u})$ *is the score function which is given by*

$$\boldsymbol{\rho}(\mathbf{u}) = \nabla \log f_U(\mathbf{u}) = \begin{bmatrix} \frac{\partial \log f_U(\mathbf{u})}{\partial u_1} & \dots & \frac{\partial \log f_U(\mathbf{u})}{\partial u_n} \end{bmatrix}^\top \tag{111}$$

Since we are mainly interested in the additive Gaussian channel, how the Fisher information matrix behaves under the addition of two independent random vectors is crucial. Regarding this, we have the following lemma which is due to [39].

**Lemma 5 ([39])** *Let* $\mathbf{U}$ *be a random vector with differentiable density, and let* $\boldsymbol{\Sigma}_U \succ \mathbf{0}$ *be its covariance matrix. Moreover, let* $\mathbf{V}$ *be another random vector with differentiable density, and be independent of* $\mathbf{U}$*. Then, we have the following facts:*

1. *Matrix form of the Cramer-Rao inequality*

$$\mathbf{J}(\mathbf{U}) \succeq \boldsymbol{\Sigma}_U^{-1} \tag{112}$$

   *which is satisfied with equality if* $\mathbf{U}$ *is Gaussian.*

2. *For any square matrix* $\mathbf{A}$,

$$\mathbf{J}(\mathbf{U}+\mathbf{V}) \preceq \mathbf{A}\mathbf{J}(\mathbf{U})\mathbf{A}^\top + (\mathbf{I}-\mathbf{A})\mathbf{J}(\mathbf{V})(\mathbf{I}-\mathbf{A})^\top \tag{113}$$

We will use the following consequences of this lemma.

**Corollary 2** *Let* $\mathbf{U}, \mathbf{V}$ *be as specified before. Then,*

1. $\mathbf{J}(\mathbf{U}+\mathbf{V}) \preceq \mathbf{J}(\mathbf{U})$
2. $\mathbf{J}(\mathbf{U}+\mathbf{V}) \preceq \left[\mathbf{J}(\mathbf{U})^{-1} + \mathbf{J}(\mathbf{V})^{-1}\right]^{-1}$

**Proof:** The first part of the corollary is obtained by choosing $\mathbf{A} = \mathbf{I}$, and the second part is obtained by choosing

$$\mathbf{A} = \left[\mathbf{J}(\mathbf{U})^{-1} + \mathbf{J}(\mathbf{V})^{-1}\right]^{-1}\mathbf{J}(\mathbf{U})^{-1} \tag{114}$$

and also by noting that $\mathbf{J}(\cdot)$ is always a symmetric matrix. ■

The following lemma regarding the Fisher information matrix is also useful in the proof of Theorem 4.

**Lemma 6** *Let $\mathbf{U}, \mathbf{V}_1, \mathbf{V}_2$ be random vectors such that $\mathbf{U}$ and $(\mathbf{V}_1, \mathbf{V}_2)$ are independent. Moreover, let $\mathbf{V}_1, \mathbf{V}_2$ be Gaussian random vectors with covariance matrices $\mathbf{0} \prec \mathbf{\Sigma}_1 \preceq \mathbf{\Sigma}_2$. Then, we have*

$$\mathbf{J}(\mathbf{U}+\mathbf{V}_2)^{-1} - \mathbf{\Sigma}_2 \succeq \mathbf{J}(\mathbf{U}+\mathbf{V}_1)^{-1} - \mathbf{\Sigma}_1 \tag{115}$$

**Proof:** Without loss of generality, let $\mathbf{V}_2 = \mathbf{V}_1 + \tilde{\mathbf{V}}_1$ such that $\tilde{\mathbf{V}}_1$ is a Gaussian random vector with covariance matrix $\mathbf{\Sigma}_2 - \mathbf{\Sigma}_1$, and independent of $\mathbf{V}_1$. Due to the second part of Corollary 2, we have

$$\begin{aligned}\mathbf{J}(\mathbf{U}+\mathbf{V}_2) = \mathbf{J}(\mathbf{U}+\mathbf{V}_1+\tilde{\mathbf{V}}_1) &\preceq \left[\mathbf{J}(\mathbf{U}+\mathbf{V}_1)^{-1} + \mathbf{J}(\tilde{\mathbf{V}}_1)^{-1}\right]^{-1} &(116)\\ &= \left[\mathbf{J}(\mathbf{U}+\mathbf{V}_1)^{-1} + \mathbf{\Sigma}_2 - \mathbf{\Sigma}_1\right]^{-1} &(117)\end{aligned}$$

which is equivalent to

$$\mathbf{J}(\mathbf{U}+\mathbf{V}_2)^{-1} \succeq \mathbf{J}(\mathbf{U}+\mathbf{V}_1)^{-1} + \mathbf{\Sigma}_2 - \mathbf{\Sigma}_1 \tag{118}$$

which proves the lemma. ■

Moreover, we need the relationship between the Fisher information matrix and the differential entropy, which is due to [31].

**Lemma 7 ([31])** *Let $\mathbf{X}$ and $\mathbf{N}$ be independent random vectors, where $\mathbf{N}$ is zero-mean Gaussian with covariance matrix $\mathbf{\Sigma}_N \succ \mathbf{0}$, and $\mathbf{X}$ has a finite second order moment. Then, we have*

$$\nabla_{\mathbf{\Sigma}_N} h(\mathbf{X}+\mathbf{N}) = \frac{1}{2}\mathbf{J}(\mathbf{X}+\mathbf{N}) \tag{119}$$

## 5.3 Proof of Theorem 4

To prove Theorem 4, we first consider the following expression

$$h(\mathbf{X}+\mathbf{N}_Z) - h(\mathbf{X}+\mathbf{N}_2) \tag{120}$$

which is bounded due to the covariance constraint on $\mathbf{X}$. In particular, we have

$$\frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_Z|}{|\mathbf{S}+\mathbf{\Sigma}_2|} \leq h(\mathbf{X}+\mathbf{N}_Z) - h(\mathbf{X}+\mathbf{N}_2) \leq \frac{1}{2}\log\frac{|\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_2|} \tag{121}$$

To see this, define $\tilde{\mathbf{N}}$ which is Gaussian with covariance matrix $\mathbf{\Sigma}_Z - \mathbf{\Sigma}_2$, and is independent of $\mathbf{N}_2$ and $\mathbf{X}$. Thus, without loss of generality, we can assume $\mathbf{Z} = \mathbf{X} + \mathbf{N}_2 + \tilde{\mathbf{N}}$. Then, the

left-hand side of (121) can be verified by noting that

$$h(\mathbf{X}+\mathbf{N}_Z)-h(\mathbf{X}+\mathbf{N}_2)=I(\tilde{\mathbf{N}};\mathbf{X}+\mathbf{N}_2+\tilde{\mathbf{N}}) \tag{122}$$

and then by using Lemma 4. The right-hand side of (121) follows from

$$\begin{aligned}
h(\mathbf{X}+\mathbf{N}_Z)-h(\mathbf{X}+\mathbf{N}_2) &= I(\tilde{\mathbf{N}};\mathbf{X}+\mathbf{N}_Z) && (123)\\
&= h(\tilde{\mathbf{N}})-h(\tilde{\mathbf{N}}|\mathbf{X}+\mathbf{N}_Z) && (124)\\
&\leq h(\tilde{\mathbf{N}})-h(\tilde{\mathbf{N}}|\mathbf{X}+\mathbf{N}_Z,\mathbf{X}) && (125)\\
&= h(\tilde{\mathbf{N}})-h(\tilde{\mathbf{N}}|\mathbf{N}_Z) && (126)\\
&= I(\tilde{\mathbf{N}};\mathbf{N}_Z) && (127)\\
&= \frac{1}{2}\log\frac{|\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_2|} && (128)
\end{aligned}$$

where (125) comes from the fact that conditioning cannot increase entropy, and (126) is due to the fact that $\mathbf{X}$ and $(\mathbf{N}_2,\tilde{\mathbf{N}})$ are independent. Thus, we can fix the difference of the differential entropies in (121) to an $\alpha$ in this range, i.e., we can set

$$h(\mathbf{X}+\mathbf{N}_Z)-h(\mathbf{X}+\mathbf{N}_2)=\alpha \tag{129}$$

where $\alpha\in\left[\frac{1}{2}\log|\mathbf{S}+\mathbf{\Sigma}_Z|/|\mathbf{S}+\mathbf{\Sigma}_2|,\frac{1}{2}\log|\mathbf{\Sigma}_Z|/|\mathbf{\Sigma}_2|\right]$. We now would like to understand how the constraint in (129) affects the set of admissible random vectors. For that purpose, we use Lemma 7, and express this difference of entropies as an integral of the Fisher information matrix[3]

$$\alpha=h(\mathbf{X}+\mathbf{N}_Z)-h(\mathbf{X}+\mathbf{N}_2)=\frac{1}{2}\int_{\mathbf{\Sigma}_2}^{\mathbf{\Sigma}_Z}\mathbf{J}(\mathbf{X}+\mathbf{N})d\mathbf{\Sigma}_N \tag{130}$$

Using the stability of Gaussian random vectors, we can express $\mathbf{J}(\mathbf{X}+\mathbf{N})$ as

$$\mathbf{J}(\mathbf{X}+\mathbf{N})=\mathbf{J}(\mathbf{X}+\mathbf{N}_2+\tilde{\mathbf{N}}) \tag{131}$$

where $\tilde{\mathbf{N}}$ is a zero-mean Gaussian random vector with covariance matrix $\mathbf{\Sigma}_N-\mathbf{\Sigma}_2\succeq\mathbf{0}$, and is independent of $\mathbf{N}_2$. Using the second part of Corollary 2 in (131), we get

$$\begin{aligned}
\mathbf{J}(\mathbf{X}+\mathbf{N})=\mathbf{J}(\mathbf{X}+\mathbf{N}_2+\tilde{\mathbf{N}}) &\preceq \left[\mathbf{J}(\mathbf{X}+\mathbf{N}_2)^{-1}+\mathbf{J}(\tilde{\mathbf{N}})^{-1}\right]^{-1} && (132)\\
&= \left[\mathbf{J}(\mathbf{X}+\mathbf{N}_2)^{-1}+\mathbf{\Sigma}_N-\mathbf{\Sigma}_2\right]^{-1} && (133)
\end{aligned}$$

[3]The integration in (130), i.e., $\int_{\mathbf{\Sigma}_2}^{\mathbf{\Sigma}_Z}\mathbf{J}(\cdot)d\mathbf{\Sigma}$, is a line integral of the vector-valued function $\mathbf{J}(\cdot)$. Moreover, since $\mathbf{J}(\cdot)$ is the gradient of a scalar field, the integration expressed in $\int_{\mathbf{\Sigma}_2}^{\mathbf{\Sigma}_Z}\mathbf{J}(\cdot)d\mathbf{\Sigma}$ is path-free, i.e., it yields the same value for any path from $\mathbf{\Sigma}_2$ to $\mathbf{\Sigma}_Z$. This remark applies to all upcoming integrals of $\mathbf{J}(\cdot)$.

where we used the fact that $\mathbf{J}(\tilde{\mathbf{N}}) = (\mathbf{\Sigma}_N - \mathbf{\Sigma}_2)^{-1}$ which is a consequence of the first part of Lemma 5 by noting that $\tilde{\mathbf{N}}$ is Gaussian. We now bound the integral in (130) by using (133). For that purpose, we introduce the following lemma.

**Lemma 8** *Let $\mathbf{K}_1, \mathbf{K}_2$ be positive semi-definite matrices satisfying $\mathbf{0} \preceq \mathbf{K}_1 \preceq \mathbf{K}_2$, and $\mathbf{f}(\mathbf{K})$ be a matrix-valued function such that $\mathbf{f}(\mathbf{K}) \succeq \mathbf{0}$ for $\mathbf{K}_1 \preceq \mathbf{K} \preceq \mathbf{K}_2$. Then, we have*

$$\int_{\mathbf{K}_1}^{\mathbf{K}_2} \mathbf{f}(\mathbf{K}) d\mathbf{K} \geq 0 \tag{134}$$

**Proof:** The integral is equivalent to

$$\int_{\mathbf{K}_1}^{\mathbf{K}_2} \mathbf{f}(\mathbf{K}) d\mathbf{K} = \int_0^1 \mathbf{1}^\top \left[\mathbf{f}\big(\mathbf{K}_1 + t(\mathbf{K}_2 - \mathbf{K}_1)\big) \odot (\mathbf{K}_2 - \mathbf{K}_1)\right] \mathbf{1} dt \tag{135}$$

where $\odot$ denotes the Schur (Hadamard) product, and $\mathbf{1} = [1 \ \ldots \ 1]^\top$ with appropriate size. Since the Schur product of two positive semi-definite matrices is positive semi-definite [40], the integrand is non-negative implying the non-negativity of the integral. ■

In light of this lemma, using (133) in (130), we get

$$\begin{aligned} \alpha &\leq \frac{1}{2} \int_{\mathbf{\Sigma}_2}^{\mathbf{\Sigma}_Z} \left[\mathbf{J}(\mathbf{X} + \mathbf{N}_2)^{-1} + \mathbf{\Sigma}_N - \mathbf{\Sigma}_2\right]^{-1} d\mathbf{\Sigma}_N && (136) \\ &= \frac{1}{2} \log \frac{|\mathbf{J}(\mathbf{X} + \mathbf{N}_2)^{-1} + \mathbf{\Sigma}_Z - \mathbf{\Sigma}_2|}{|\mathbf{J}(\mathbf{X} + \mathbf{N}_2)^{-1}|} && (137) \end{aligned}$$

where we used the well-known fact that $\nabla_{\mathbf{\Sigma}} \log |\mathbf{\Sigma}| = \mathbf{\Sigma}^{-\top}$ for $\mathbf{\Sigma} \succ \mathbf{0}$. We also note that the denominator in (137) is strictly positive because

$$\mathbf{J}(\mathbf{X} + \mathbf{N}_2)^{-1} \succeq \mathbf{J}(\mathbf{N}_2)^{-1} = \mathbf{\Sigma}_2 \succ \mathbf{0} \tag{138}$$

which implies $|\mathbf{J}(\mathbf{X} + \mathbf{N}_2)^{-1}| > 0$.

Following similar steps, we can also find a lower bound on $\alpha$. Again, using the stability of Gaussian random vectors, we have

$$\mathbf{J}(\mathbf{X} + \mathbf{N}_Z) = \mathbf{J}(\mathbf{X} + \mathbf{N} + \tilde{\mathbf{N}}) \tag{139}$$

where $\mathbf{N}, \tilde{\mathbf{N}}$ are zero-mean Gaussian random vectors with covariance matrices $\mathbf{\Sigma}_N, \mathbf{\Sigma}_Z - \mathbf{\Sigma}_N$, respectively, $\mathbf{\Sigma}_2 \preceq \mathbf{\Sigma}_N \preceq \mathbf{\Sigma}_Z$, and they are independent. Using the second part of Corollary 2 in (139) yields

$$\begin{aligned} \mathbf{J}(\mathbf{X} + \mathbf{N}_Z) = \mathbf{J}(\mathbf{X} + \mathbf{N} + \tilde{\mathbf{N}}) &\preceq \left[\mathbf{J}(\mathbf{X} + \mathbf{N})^{-1} + \mathbf{J}(\tilde{\mathbf{N}})^{-1}\right]^{-1} && (140) \\ &= \left[\mathbf{J}(\mathbf{X} + \mathbf{N})^{-1} + \mathbf{\Sigma}_Z - \mathbf{\Sigma}_N\right]^{-1} && (141) \end{aligned}$$

where we used the fact that $\mathbf{J}(\tilde{\mathbf{N}}) = (\boldsymbol{\Sigma}_Z - \boldsymbol{\Sigma}_N)^{-1}$ which follows from the first part of Lemma 5 due to the Gaussianity of $\tilde{\mathbf{N}}$. Then, (141) is equivalent to

$$\mathbf{J}(\mathbf{X}+\mathbf{N}_Z)^{-1} \succeq \mathbf{J}(\mathbf{X}+\mathbf{N})^{-1} + \boldsymbol{\Sigma}_Z - \boldsymbol{\Sigma}_N \tag{142}$$

and that implies

$$\left[\mathbf{J}(\mathbf{X}+\mathbf{N}_Z)^{-1} + \boldsymbol{\Sigma}_N - \boldsymbol{\Sigma}_Z\right]^{-1} \preceq \mathbf{J}(\mathbf{X}+\mathbf{N}) \tag{143}$$

Use of Lemma 8 and (143) in (130) yields

$$\begin{aligned}
\alpha &\geq \int_{\boldsymbol{\Sigma}_2}^{\boldsymbol{\Sigma}_Z} \left[\mathbf{J}(\mathbf{X}+\mathbf{N}_Z)^{-1} + \boldsymbol{\Sigma}_N - \boldsymbol{\Sigma}_Z\right]^{-1} d\boldsymbol{\Sigma}_N && (144)\\
&= \frac{1}{2}\log\frac{|\mathbf{J}(\mathbf{X}+\mathbf{N}_Z)^{-1}|}{|\mathbf{J}(\mathbf{X}+\mathbf{N}_Z)^{-1} + \boldsymbol{\Sigma}_2 - \boldsymbol{\Sigma}_Z|} && (145)
\end{aligned}$$

where we again used $\nabla_{\boldsymbol{\Sigma}} \log|\boldsymbol{\Sigma}| = \boldsymbol{\Sigma}^{-\top}$ for $\boldsymbol{\Sigma} \succ \mathbf{0}$. Here also, the denominator is strictly positive because

$$\mathbf{J}(\mathbf{X}+\mathbf{N}_Z)^{-1} + \boldsymbol{\Sigma}_2 - \boldsymbol{\Sigma}_Z \succeq \mathbf{J}(\mathbf{N}_Z)^{-1} + \boldsymbol{\Sigma}_2 - \boldsymbol{\Sigma}_Z = \boldsymbol{\Sigma}_2 \succ \mathbf{0} \tag{146}$$

which implies $|\mathbf{J}(\mathbf{X}+\mathbf{N}_Z)^{-1} + \boldsymbol{\Sigma}_2 - \boldsymbol{\Sigma}_Z| > 0$. Combining the two bounds on $\alpha$ given in (137) and (145) yields

$$\frac{1}{2}\log\frac{|\mathbf{J}(\mathbf{X}+\mathbf{N}_Z)^{-1}|}{|\mathbf{J}(\mathbf{X}+\mathbf{N}_Z)^{-1} + \boldsymbol{\Sigma}_2 - \boldsymbol{\Sigma}_Z|} \leq \alpha \leq \frac{1}{2}\log\frac{|\mathbf{J}(\mathbf{X}+\mathbf{N}_2)^{-1} + \boldsymbol{\Sigma}_Z - \boldsymbol{\Sigma}_2|}{|\mathbf{J}(\mathbf{X}+\mathbf{N}_2)^{-1}|} \tag{147}$$

Next, we will discuss the implications of (147). First, we have a digression of technical nature to provide the necessary information for such a discussion. We present the following lemma from [40].

**Lemma 9 ([40], Theorem 7.6.4, page 465)** *Let $\mathbf{A}, \mathbf{B} \in M_n$, where $M_n$ is the set of all square matrices of size $n \times n$ over the complex numbers, be two Hermitian matrices and suppose that there is a real linear combination of $\mathbf{A}$ and $\mathbf{B}$ that is positive definite. Then there exists a non-singular matrix $\mathbf{C}$ such that both $\mathbf{C}^H\mathbf{A}\mathbf{C}$ and $\mathbf{C}^H\mathbf{B}\mathbf{C}$ are diagonal, where $(\cdot)^H$ denotes the conjugate transpose.*

**Lemma 10** *Consider the function*

$$r(t) = \frac{1}{2}\log\frac{|\mathbf{A}+\mathbf{B}+t\boldsymbol{\Delta}|}{|\mathbf{A}+t\boldsymbol{\Delta}|}, \qquad 0 \leq t \leq 1 \tag{148}$$

*where $\mathbf{A}, \mathbf{B}, \boldsymbol{\Delta}$ are real, symmetric matrices, and $\mathbf{A} \succ \mathbf{0}$, $\mathbf{B} \succeq \mathbf{0}, \boldsymbol{\Delta} \succeq \mathbf{0}$. The function $r(t)$ is continuous and monotonically decreasing in $t$.*

**Proof:** We first define the function inside the $\log(\cdot)$ as

$$f(t) = \frac{|\mathbf{A} + \mathbf{B} + t\boldsymbol{\Delta}|}{|\mathbf{A} + t\boldsymbol{\Delta}|}, \qquad 0 \leq t \leq 1 \tag{149}$$

We first prove the continuity of $r(t)$. To this end, consider the function

$$g(t) = |\mathbf{E} + t\boldsymbol{\Delta}|, \qquad 0 \leq t \leq 1 \tag{150}$$

where $\mathbf{E} \succ \mathbf{0}$ is a real, symmetric matrix. By Lemma 9, there exists a non-singular matrix $\mathbf{C}$ such that both $\mathbf{C}^\top \mathbf{E} \mathbf{C}$ and $\mathbf{C}^\top \boldsymbol{\Delta} \mathbf{C}$ are diagonal. Thus, using this fact, we get

$$g(t) = \left|\mathbf{C}^{-\top}\mathbf{C}^\top \mathbf{E}\mathbf{C}\mathbf{C}^{-1} + t\mathbf{C}^{-\top}\mathbf{C}^\top \boldsymbol{\Delta}\mathbf{C}\mathbf{C}^{-1}\right| \tag{151}$$

$$= \left|\mathbf{C}^{-\top}\right| \left|\mathbf{C}^\top \mathbf{E}\mathbf{C} + t\mathbf{C}^\top \boldsymbol{\Delta}\mathbf{C}\right| \left|\mathbf{C}^{-1}\right| \tag{152}$$

$$= \frac{1}{|\mathbf{C}|^2} \left|\mathbf{C}^\top \mathbf{E}\mathbf{C} + t\mathbf{C}^\top \boldsymbol{\Delta}\mathbf{C}\right| \tag{153}$$

$$= \frac{1}{|\mathbf{C}|^2} |\mathbf{D}_E + t\mathbf{D}_\Delta| \tag{154}$$

where (152) follows from the fact that $|\mathbf{AB}| = |\mathbf{A}||\mathbf{B}|$, (153) comes from the fact that $\left|\mathbf{C}^{-\top}\right| = |\mathbf{C}^{-1}| = 1/|\mathbf{C}|$, and in (154), we defined the diagonal matrices $\mathbf{D}_E = \mathbf{C}^\top \mathbf{E}\mathbf{C}$, $\mathbf{D}_\Delta = \mathbf{C}^\top \boldsymbol{\Delta}\mathbf{C}$. Let the diagonal elements of $\mathbf{D}_E$ and $\mathbf{D}_\Delta$ be $\{d_{E,i}\}_{i=1}^n$ and $\{d_{\Delta,i}\}_{i=1}^n$, respectively. Then, $g(t)$ can be expressed as

$$g(t) = \frac{1}{|\mathbf{C}|^2} \prod_{i=1}^{n} (d_{E,i} + t d_{\Delta,i}) \tag{155}$$

which is polynomial in $t$, thus $g(t)$ is continuous in $t$. Being the ratio of two non-zero continuous functions, $f(t)$ is continuous as well. Then, continuity of $r(t)$ follows from the fact that composition of two continuous functions is also continuous.

We now show the monotonicity of $r(t)$. To this end, consider the derivative of $r(t)$

$$\frac{dr(t)}{dt} = \frac{1}{2f(t)} \frac{df(t)}{dt} \tag{156}$$

where we have $f(t) > 0$ because of the facts that $\mathbf{A} \succ \mathbf{0}$, $\mathbf{B} \succeq \mathbf{0}, \boldsymbol{\Delta} \succeq \mathbf{0}$, and $0 \leq t \leq 1$. Moreover, $f(t)$ is monotonically decreasing in $t$, which can be deduced from (100), implying $df(t)/dt \leq 0$. Thus, we have $dr(t)/dt \leq 0$, completing the proof. ■

After this digression, we are ready to investigate the implications of (147). For that purpose, let us select $\mathbf{A}, \mathbf{B}, \boldsymbol{\Delta}$ in $r(t)$ in Lemma 10 as follows

$$\mathbf{A} = \mathbf{J}(\mathbf{X}+\mathbf{N}_2)^{-1} \tag{157}$$
$$\mathbf{B} = \boldsymbol{\Sigma}_Z - \boldsymbol{\Sigma}_2 \tag{158}$$
$$\boldsymbol{\Delta} = \mathbf{J}(\mathbf{X}+\mathbf{N}_Z)^{-1} + \boldsymbol{\Sigma}_2 - \boldsymbol{\Sigma}_Z - \mathbf{J}(\mathbf{X}+\mathbf{N}_2)^{-1} \tag{159}$$

where clearly $\mathbf{A} \succ \mathbf{0}$, $\mathbf{B} \succeq \mathbf{0}$, and also $\boldsymbol{\Delta} \succeq \mathbf{0}$ due to Lemma 6. With these selections, we have

$$r(0) = \frac{1}{2}\log\frac{|\mathbf{J}(\mathbf{X}+\mathbf{N}_2)^{-1} + \boldsymbol{\Sigma}_Z - \boldsymbol{\Sigma}_2|}{|\mathbf{J}(\mathbf{X}+\mathbf{N}_2)^{-1}|} \tag{160}$$
$$r(1) = \frac{1}{2}\log\frac{|\mathbf{J}(\mathbf{X}+\mathbf{N}_Z)^{-1}|}{|\mathbf{J}(\mathbf{X}+\mathbf{N}_Z)^{-1} + \boldsymbol{\Sigma}_2 - \boldsymbol{\Sigma}_Z|} \tag{161}$$

Thus, (147) can be expressed as

$$r(1) \leq \alpha \leq r(0) \tag{162}$$

We know from Lemma 10 that $r(t)$ is continuous in $t$. Then, from the intermediate value theorem, there exists a $t^*$ such that $r(t^*) = \alpha$. Thus, we have

$$\alpha = r(t^*) = \frac{1}{2}\log\frac{|\mathbf{A} + t^*\boldsymbol{\Delta} + \boldsymbol{\Sigma}_Z - \boldsymbol{\Sigma}_2|}{|\mathbf{A}+t^*\boldsymbol{\Delta}|} \tag{163}$$
$$= \frac{1}{2}\log\frac{|\mathbf{K}^* + \boldsymbol{\Sigma}_Z|}{|\mathbf{K}^* + \boldsymbol{\Sigma}_2|} \tag{164}$$

where $\mathbf{K}^* = \mathbf{A} + t^*\boldsymbol{\Delta} - \boldsymbol{\Sigma}_2$. Since $0 \leq t^* \leq 1$, $\mathbf{K}^*$ satisfies the following orderings,

$$\mathbf{J}(\mathbf{X}+\mathbf{N}_2)^{-1} - \boldsymbol{\Sigma}_2 \preceq \mathbf{K}^* \preceq \mathbf{J}(\mathbf{X}+\mathbf{N}_Z)^{-1} - \boldsymbol{\Sigma}_Z \tag{165}$$

which in turn, by using Lemma 5 and Corollary 2, imply the following orderings,

$$\mathbf{K}^* \succeq \mathbf{J}(\mathbf{X}+\mathbf{N}_2)^{-1} - \boldsymbol{\Sigma}_2 \succeq \mathbf{J}(\mathbf{N}_2)^{-1} - \boldsymbol{\Sigma}_2 = \boldsymbol{\Sigma}_2 - \boldsymbol{\Sigma}_2 = \mathbf{0} \tag{166}$$
$$\mathbf{K}^\star \preceq \mathbf{J}(\mathbf{X}+\mathbf{N}_Z)^{-1} - \boldsymbol{\Sigma}_Z \preceq \mathrm{Cov}(\mathbf{X}) + \boldsymbol{\Sigma}_Z - \boldsymbol{\Sigma}_Z = \mathrm{Cov}(\mathbf{X}) \preceq \mathbf{S} \tag{167}$$

which can be summarized as follows,

$$\mathbf{0} \preceq \mathbf{K}^\star \preceq \mathbf{S} \tag{168}$$

In addition, using Lemma 6 in (165), we get

$$\mathbf{K}^* \succeq \mathbf{J}(\mathbf{X}+\mathbf{N})^{-1} - \boldsymbol{\Sigma}_N \tag{169}$$

for any Gaussian random vector $\mathbf{N}$ such that its covariance matrix satisfies $\mathbf{\Sigma}_N \preceq \mathbf{\Sigma}_2$. The inequality in (169) is equivalent to

$$\mathbf{J}(\mathbf{X}+\mathbf{N}) \succeq (\mathbf{K}^* + \mathbf{\Sigma}_N)^{-1}, \quad \text{for} \quad \mathbf{\Sigma}_N \preceq \mathbf{\Sigma}_2 \tag{170}$$

where $\mathbf{N}$ is a Gaussian random vector with covariance matrix $\mathbf{\Sigma}_N$.

Returning to the proof of Theorem 4, we now lower bound

$$h(\mathbf{X}+\mathbf{N}_Z) - (\mathbf{X}+\mathbf{N}_1) \tag{171}$$

while keeping

$$h(\mathbf{X}+\mathbf{N}_Z) - (\mathbf{X}+\mathbf{N}_2) = \alpha = \frac{1}{2}\log\frac{|\mathbf{K}^*+\mathbf{\Sigma}_Z|}{|\mathbf{K}^*+\mathbf{\Sigma}_2|} \tag{172}$$

The lower bound on (171) can be obtained as follows

$$\begin{aligned}
h(\mathbf{X}+\mathbf{N}_Z) - h(\mathbf{X}+\mathbf{N}_1) &= \frac{1}{2}\int_{\mathbf{\Sigma}_1}^{\mathbf{\Sigma}_Z} \mathbf{J}(\mathbf{X}+\mathbf{N}) d\mathbf{\Sigma}_N & (173)\\
&= \frac{1}{2}\int_{\mathbf{\Sigma}_1}^{\mathbf{\Sigma}_2} \mathbf{J}(\mathbf{X}+\mathbf{N}) d\mathbf{\Sigma}_N + \frac{1}{2}\int_{\mathbf{\Sigma}_2}^{\mathbf{\Sigma}_Z} \mathbf{J}(\mathbf{X}+\mathbf{N}) d\mathbf{\Sigma}_N & (174)\\
&= \frac{1}{2}\int_{\mathbf{\Sigma}_1}^{\mathbf{\Sigma}_2} \mathbf{J}(\mathbf{X}+\mathbf{N}) d\mathbf{\Sigma}_N + \frac{1}{2}\log\frac{|\mathbf{K}^*+\mathbf{\Sigma}_Z|}{|\mathbf{K}^*+\mathbf{\Sigma}_2|} & (175)\\
&\geq \frac{1}{2}\int_{\mathbf{\Sigma}_1}^{\mathbf{\Sigma}_2} (\mathbf{K}^*+\mathbf{\Sigma}_N)^{-1} d\mathbf{\Sigma}_N + \frac{1}{2}\log\frac{|\mathbf{K}^*+\mathbf{\Sigma}_Z|}{|\mathbf{K}^*+\mathbf{\Sigma}_2|} & (176)\\
&= \frac{1}{2}\log\frac{|\mathbf{K}^*+\mathbf{\Sigma}_2|}{|\mathbf{K}^*+\mathbf{\Sigma}_1|} + \frac{1}{2}\log\frac{|\mathbf{K}^*+\mathbf{\Sigma}_Z|}{|\mathbf{K}^*+\mathbf{\Sigma}_2|} & (177)\\
&= \frac{1}{2}\log\frac{|\mathbf{K}^*+\mathbf{\Sigma}_Z|}{|\mathbf{K}^\star+\mathbf{\Sigma}_1|} & (178)
\end{aligned}$$

where (174) follows from the fact that the integral in (173) is path-independent, and (176) is due to Lemma 8 and (170).

Thus, we have shown the following: For any admissible random vector $\mathbf{X}$, we can find a positive semi-definite matrix $\mathbf{K}^*$ such that $\mathbf{0} \preceq \mathbf{K}^* \preceq \mathbf{S}$, and

$$h(\mathbf{X}+\mathbf{N}_Z) - (\mathbf{X}+\mathbf{N}_2) = \frac{1}{2}\log\frac{|\mathbf{K}^*+\mathbf{\Sigma}_Z|}{|\mathbf{K}^*+\mathbf{\Sigma}_2|} \tag{179}$$

and

$$h(\mathbf{X}+\mathbf{N}_Z) - h(\mathbf{X}+\mathbf{N}_1) \geq \frac{1}{2}\log\frac{|\mathbf{K}^*+\mathbf{\Sigma}_Z|}{|\mathbf{K}^*+\mathbf{\Sigma}_1|} \tag{180}$$

which completes the proof of Theorem 4.

## 5.4 Proof of Theorem 5

We now adopt the proof of Theorem 4 to the setting of Theorem 5 by providing the conditional versions of the tools we have used in the proof of Theorem 4. Main ingredients of the proof of Theorem 4 are: the relationship between the differential entropy and the Fisher information matrix given in Lemma 7, and the properties of the Fisher information matrix given in Lemmas 5, 6 and Corollary 2. Thus, in this section, we basically provide the extensions of Lemmas 5, 6, 7 and Corollary 2 to the conditional setting. From another point of view, the material that we present in this section can be regarded as extending some well-known results on the Fisher information matrix [36, 39] to a conditional setting.

We start with the definition of the conditional Fisher information matrix.

**Definition 3** *Let* $(\mathbf{U}, \mathbf{X})$ *be an arbitrarily correlated length-n random vector pair with well-defined densities. The conditional Fisher information matrix of* $\mathbf{X}$ *given* $\mathbf{U}$ *is defined as*

$$\mathbf{J}(\mathbf{X}|\mathbf{U}) = E\left[\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})^\top\right] \tag{181}$$

*where the expectation is over the joint density* $f(\mathbf{u}, \mathbf{x})$*, and the conditional score function* $\boldsymbol{\rho}(\mathbf{x}|\mathbf{u})$ *is*

$$\boldsymbol{\rho}(\mathbf{x}|\mathbf{u}) = \nabla \log f(\mathbf{x}|\mathbf{u}) = \left[\begin{array}{ccc} \frac{\partial \log f(\mathbf{x}|\mathbf{u})}{\partial x_1} & \ldots & \frac{\partial \log f(\mathbf{x}|\mathbf{u})}{\partial x_n} \end{array}\right]^\top \tag{182}$$

The following lemma extends Stein identity [36, 39] to a conditional setting. We provide its proof in Appendix A.

**Lemma 11 (Conditional Stein Identity)** *Let* $\mathbf{U}, \mathbf{X}$ *be as specified above. Consider a smooth scalar-valued function of* $\mathbf{x}$*,* $g(\mathbf{x})$*, which well-behaves at infinity in the sense that*

$$\lim_{x_i \to \pm\infty} g(\mathbf{x}) f(\mathbf{x}|\mathbf{u}) = 0, \qquad i = 1, \ldots, n \tag{183}$$

*For such a* $g(\mathbf{x})$*, we have*

$$E\left[g(\mathbf{X})\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})\right] = -E\left[\nabla g(\mathbf{X})\right] \tag{184}$$

The following implications of this lemma are important for the upcoming proofs.

**Corollary 3** *Let* $\mathbf{U}, \mathbf{X}$ *be as specified above.*

1. $E\left[\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})\right] = \mathbf{0}$
2. $E\left[\mathbf{X}\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})^\top\right] = -\mathbf{I}$

**Proof:** The first and the second parts of the corollary follow from the previous lemma by selecting $g(\mathbf{x}) = 1$ and $g(\mathbf{x}) = x_i$, respectively. ■

We also need the following variation of this corollary whose proof is given in Appendix B.

**Lemma 12** *Let* $\mathbf{U}, \mathbf{X}$ *be as specified above. Then, we have*

1. $E\left[\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})|\mathbf{U}\right] = \mathbf{0}$.

2. *Let* $g(\mathbf{u})$ *be a finite, scalar-valued function of* $\mathbf{u}$. *For such a* $g(\mathbf{u})$, *we have*

$$E\left[g(\mathbf{U})\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})\right] = \mathbf{0} \tag{185}$$

3. *Let* $E\left[\mathbf{X}|\mathbf{U}\right]$ *be finite, then we have*

$$E\left[E\left[\mathbf{X}|\mathbf{U}\right]\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})^\top\right] = \mathbf{0} \tag{186}$$

We are now ready to prove the conditional version of the Cramer-Rao inequality, i.e., the generalization of the first part of Lemma 5 to a conditional setting.

**Lemma 13 (Conditional Cramer-Rao Inequality)** *Let* $\mathbf{U}, \mathbf{X}$ *be arbitrarily correlated random vectors with well-defined densities. Let the conditional covariance matrix of* $\mathbf{X}$ *be* $\mathrm{Cov}(\mathbf{X}|\mathbf{U}) \succ \mathbf{0}$, *then we have*

$$\mathbf{J}(\mathbf{X}|\mathbf{U}) \succeq \mathrm{Cov}(\mathbf{X}|\mathbf{U})^{-1} \tag{187}$$

*which is satisfied with equality if* $(\mathbf{U}, \mathbf{X})$ *is jointly Gaussian with conditional covariance matrix* $\mathrm{Cov}(\mathbf{X}|\mathbf{U})$.

**Proof:** We first prove the inequality

$$\begin{aligned}
\mathbf{0} \preceq E\Bigg[&\Big(\boldsymbol{\rho}(\mathbf{X}|\mathbf{U}) + \mathrm{Cov}(\mathbf{X}|\mathbf{U})^{-1}\big(\mathbf{X} - E\left[\mathbf{X}|\mathbf{U}\right]\big)\Big) \\
&\qquad\Big(\boldsymbol{\rho}(\mathbf{X}|\mathbf{U}) + \mathrm{Cov}(\mathbf{X}|\mathbf{U})^{-1}\big(\mathbf{X} - E\left[\mathbf{X}|\mathbf{U}\right]\big)\Big)^\top\Bigg] && (188)\\
&= E\left[\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})^\top\right] + E\left[\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})\big(\mathbf{X} - E\left[\mathbf{X}|\mathbf{U}\right]\big)^\top\right]\mathrm{Cov}(\mathbf{X}|\mathbf{U})^{-1} \\
&\quad + \mathrm{Cov}(\mathbf{X}|\mathbf{U})^{-1}E\left[\big(\mathbf{X} - E\left[\mathbf{X}|\mathbf{U}\right]\big)\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})^\top\right] \\
&\quad + \mathrm{Cov}(\mathbf{X}|\mathbf{U})^{-1}E\left[\big(\mathbf{X} - E\left[\mathbf{X}|\mathbf{U}\right]\big)\big(\mathbf{X} - E\left[\mathbf{X}|\mathbf{U}\right]\big)^\top\right]\mathrm{Cov}(\mathbf{X}|\mathbf{U})^{-1} && (189)\\
&= \mathbf{J}(\mathbf{X}|\mathbf{U}) + E\left[\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})\big(\mathbf{X} - E\left[\mathbf{X}|\mathbf{U}\right]\big)^\top\right]\mathrm{Cov}(\mathbf{X}|\mathbf{U})^{-1} \\
&\quad + \mathrm{Cov}(\mathbf{X}|\mathbf{U})^{-1}E\left[\big(\mathbf{X} - E\left[\mathbf{X}|\mathbf{U}\right]\big)\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})^\top\right] + \mathrm{Cov}(\mathbf{X}|\mathbf{U})^{-1} && (190)
\end{aligned}$$

where for the second equality, we used the definition of the conditional Fisher information matrix, and the conditional covariance matrix. We note that

$$\left(E\left[\left(\mathbf{X}-E\left[\mathbf{X}|\mathbf{U}\right]\right)\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})^\top\right]\right)^\top = E\left[\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})\left(\mathbf{X}-E\left[\mathbf{X}|\mathbf{U}\right]\right)^\top\right] \tag{191}$$

$$= E\left[\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})\mathbf{X}^\top\right] - E\left[\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})E\left[\mathbf{X}|\mathbf{U}\right]^\top\right] \tag{192}$$

$$= E\left[\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})\mathbf{X}^\top\right] \tag{193}$$

$$= -\mathbf{I} \tag{194}$$

where (193) is due to the third part of Lemma 12, and (194) is a result of the second part of Corollary 3. Using (194) in (190) gives

$$\mathbf{0} \preceq \mathbf{J}(\mathbf{X}|\mathbf{U}) - \mathrm{Cov}(\mathbf{X}|\mathbf{U})^{-1} - \mathrm{Cov}(\mathbf{X}|\mathbf{U})^{-1} + \mathrm{Cov}(\mathbf{X}|\mathbf{U})^{-1} \tag{195}$$

which concludes the proof.

For the equality case, consider the conditional Gaussian distribution

$$f(\mathbf{x}|\mathbf{u}) = C\exp\left(-\frac{1}{2}\left(\mathbf{x}-E\left[\mathbf{X}|\mathbf{U}=\mathbf{u}\right]\right)^\top\mathrm{Cov}(\mathbf{X}|\mathbf{U})^{-1}\left(\mathbf{x}-E\left[\mathbf{X}|\mathbf{U}=\mathbf{u}\right]\right)\right) \tag{196}$$

where $C$ is the normalizing factor. The conditional score function is

$$\boldsymbol{\rho}(\mathbf{x}|\mathbf{u}) = -\mathrm{Cov}(\mathbf{X}|\mathbf{U})^{-1}\left(\mathbf{x}-E\left[\mathbf{X}|\mathbf{U}=\mathbf{u}\right]\right) \tag{197}$$

which implies $\mathbf{J}(\mathbf{X}|\mathbf{U}) = \mathrm{Cov}(\mathbf{X}|\mathbf{U})^{-1}$. ■

We now present the conditional convolution identity which is crucial to extend the second part of Lemma 5 to a conditional setting.

**Lemma 14 (Conditional Convolution Identity)** *Let $\mathbf{X},\mathbf{Y},\mathbf{U}$ be length-$n$ random vectors and let the density for any combination of these random vectors exist. Moreover, let $\mathbf{X}$ and $\mathbf{Y}$ be conditionally independent given $\mathbf{U}$, and let $\mathbf{W}$ be defined as $\mathbf{W}=\mathbf{X}+\mathbf{Y}$. Then, we have*

$$\boldsymbol{\rho}(\mathbf{w}|\mathbf{u}) = E\left[\boldsymbol{\rho}(\mathbf{X}|\mathbf{U}=\mathbf{u})|\mathbf{W}=\mathbf{w},\mathbf{U}=\mathbf{u}\right] = E\left[\boldsymbol{\rho}(\mathbf{Y}|\mathbf{U}=\mathbf{u})|\mathbf{W}=\mathbf{w},\mathbf{U}=\mathbf{u}\right] \tag{198}$$

The proof of this lemma is given in Appendix C. We will use this lemma to prove the conditional Fisher information matrix inequality, i.e., the generalization of the second part of Lemma 5.

**Lemma 15 (Conditional Fisher Information Matrix Inequality)** *Let $\mathbf{X},\mathbf{Y},\mathbf{U}$ be as*

*specified in the previous lemma. For any square matrix* $\mathbf{A}$*, we have*

$$\mathbf{J}(\mathbf{X}+\mathbf{Y}|\mathbf{U}) \preceq \mathbf{A}\mathbf{J}(\mathbf{X}|\mathbf{U})\mathbf{A}^\top + (\mathbf{I}-\mathbf{A})\,\mathbf{J}(\mathbf{Y}|\mathbf{U})\,(\mathbf{I}-\mathbf{A})^\top \tag{199}$$

The proof of this lemma is given in Appendix D. The following implications of Lemma 15 correspond to the conditional version of Corollary 2.

**Corollary 4** *Let* $\mathbf{X}, \mathbf{Y}, \mathbf{U}$ *be as specified in the previous lemma. Then, we have*

1. $\mathbf{J}(\mathbf{X}+\mathbf{Y}|\mathbf{U}) \preceq \mathbf{J}(\mathbf{X}|\mathbf{U})$
2. $\mathbf{J}(\mathbf{X}+\mathbf{Y}|\mathbf{U}) \preceq \left[\mathbf{J}(\mathbf{X}|\mathbf{U})^{-1} + \mathbf{J}(\mathbf{Y}|\mathbf{U})^{-1}\right]^{-1}$

**Proof:** The first part of the corollary can be obtained by setting $\mathbf{A} = \mathbf{I}$ in the previous lemma. For the second part, the selection $\mathbf{A} = \left[\mathbf{J}(\mathbf{X}|\mathbf{U})^{-1} + \mathbf{J}(\mathbf{Y}|\mathbf{U})^{-1}\right]^{-1}\mathbf{J}(\mathbf{X}|\mathbf{U})^{-1}$ yields the desired result. ■

Using this corollary, one can prove the conditional version of Lemma 6 as well, which is omitted. So far, we have proved the conditional versions of the inequalities related to the Fisher information matrix, that were used in the proof of Theorem 4. To claim that the proof of Theorem 4 can be adapted for Theorem 5, we only need the conditional version of Lemma 7. In [31], the following result is implicity present.

**Lemma 16** *Let* $(\mathbf{U}, \mathbf{X})$ *be an arbitrarily correlated random vector pair with finite second order moments, and be independent of the random vector* $\mathbf{N}$ *which is zero-mean Gaussian with covariance matrix* $\mathbf{\Sigma}_N \succ \mathbf{0}$*. Then, we have*

$$\nabla_{\mathbf{\Sigma}_N} h(\mathbf{X}+\mathbf{N}|\mathbf{U}) = \frac{1}{2}\mathbf{J}(\mathbf{X}+\mathbf{N}|\mathbf{U}) \tag{200}$$

**Proof:** Let $F_U(\mathbf{u})$ be the cumulative distribution function of $\mathbf{U}$, and $f(\mathbf{x}+\mathbf{n}|\mathbf{U}=\mathbf{u})$ be the conditional density of $\mathbf{X}+\mathbf{N}$ which is guaranteed to exist because $\mathbf{N}$ is Gaussian. We have

$$\nabla_{\mathbf{\Sigma}_N} h(\mathbf{X}+\mathbf{N}|\mathbf{U}) = \nabla_{\mathbf{\Sigma}_N} \int h(\mathbf{X}+\mathbf{N}|\mathbf{U}=\mathbf{u})dF_U(\mathbf{u}) \tag{201}$$

$$= \int \nabla_{\mathbf{\Sigma}_N} h(\mathbf{X}+\mathbf{N}|\mathbf{U}=\mathbf{u})dF_U(\mathbf{u}) \tag{202}$$

$$= \frac{1}{2}\int E\left[\nabla \log f(\mathbf{X}+\mathbf{N}|\mathbf{U}=\mathbf{u})\nabla \log f(\mathbf{X}+\mathbf{N}|\mathbf{U}=\mathbf{u})^\top\right] dF_U(\mathbf{u}) \tag{203}$$

$$= \frac{1}{2}E\left[\nabla \log f(\mathbf{X}+\mathbf{N}|\mathbf{U})\nabla \log f(\mathbf{X}+\mathbf{N}|\mathbf{U})^\top\right] \tag{204}$$

$$= \frac{1}{2}\mathbf{J}(\mathbf{X}+\mathbf{N}|\mathbf{U}) \tag{205}$$

where in (202), we changed the order of integration and differentiation, which can be done due to the finiteness of the conditional differential entropy, which in turn is ensured by the finite second-order moments of $(\mathbf{U}, \mathbf{X})$, (203) is a consequence of Lemma 7, and (205) follows from the definition of the conditional Fisher information matrix. ■

Since we have derived all necessary tools, namely conditional counterparts of Lemmas 5, 6, 7 and Corollary 2, the proof Theorem 4 can be adapted to prove Theorem 5.

## 5.5 Proof of Theorem 3 for Arbitrary $K$

We now prove Theorem 3 for arbitrary $K$. To this end, we will mainly use the intuition gained in the proof of Theorem 4 and the tools developed in the previous section. The only new ingredient that is needed is the following lemma whose proof is given in Appendix E.

**Lemma 17** *Let $(\mathbf{V}, \mathbf{U}, \mathbf{X})$ be length-$n$ random vectors with well-defined densities. Moreover, assume that the partial derivatives of $f(\mathbf{u}|\mathbf{v}, \mathbf{x})$ with respect to $x_i$, $i = 1, \ldots, n$, exist and satisfy*

$$\max_{1\leq i\leq n} \left| \frac{\partial f(\mathbf{u}|\mathbf{x}, \mathbf{v})}{\partial x_i} \right| \leq g(\mathbf{u}) \tag{206}$$

*for some integrable function $g(\mathbf{u})$. Then, if $(\mathbf{V}, \mathbf{U}, \mathbf{X})$ satisfy the Markov chain $\mathbf{V} \to \mathbf{U} \to \mathbf{X}$, we have*

$$\mathbf{J}(\mathbf{X}|\mathbf{U}) \succeq \mathbf{J}(\mathbf{X}|\mathbf{V}) \tag{207}$$

We now start the proof of Theorem 3 for arbitrary $K$. First, we rewrite the bound given in Theorem 1 for the $K$th user's secrecy rate as follows

$$I(U_K; \mathbf{Y}_K) - I(U_K; \mathbf{Z}) = I(\mathbf{X}; \mathbf{Y}_K) - I(\mathbf{X}; \mathbf{Z}) - [I(\mathbf{X}; \mathbf{Y}_K|U_K) - I(\mathbf{X}; \mathbf{Z}|U_K)] \tag{208}$$

$$\leq \frac{1}{2} \log \frac{|\mathbf{S} + \mathbf{\Sigma}_K|}{|\mathbf{\Sigma}_K|} - \frac{1}{2} \log \frac{|\mathbf{S} + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} - [I(\mathbf{X}; \mathbf{Y}_K|U_K) - I(\mathbf{X}; \mathbf{Z}|U_K)] \tag{209}$$

where in (208), we used the Markov chain $U_K \to \mathbf{X} \to (\mathbf{Y}_K, \mathbf{Z})$, and obtained (209) using the worst additive noise lemma given in Lemma 4. Moreover, using the Markov chain $U_K \to \mathbf{X} \to \mathbf{Y}_K \to \mathbf{Z}$, the other difference term in (209) can be bounded as follows.

$$0 \leq I(\mathbf{X}; \mathbf{Y}_K|U_K) - I(\mathbf{X}; \mathbf{Z}|U_K) \leq I(\mathbf{X}; \mathbf{Y}_K) - I(\mathbf{X}; \mathbf{Z}) \tag{210}$$

$$\leq \frac{1}{2} \log \frac{|\mathbf{S} + \mathbf{\Sigma}_K|}{|\mathbf{\Sigma}_K|} - \frac{1}{2} \log \frac{|\mathbf{S} + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{211}$$

The proofs of Theorems 4 and 5 reveal that for any value of $I(\mathbf{X};\mathbf{Y}_K|U_K)-I(\mathbf{X};\mathbf{Z}|U_K)$ in the range given in (211), there exists positive semi-definite matrix $\tilde{\mathbf{K}}_K$ such that

$$\mathbf{J}(\mathbf{X}+\mathbf{N}_K|U_K)^{-1}-\mathbf{\Sigma}_K \preceq \tilde{\mathbf{K}}_K \preceq \mathbf{S} \tag{212}$$

and

$$I(\mathbf{X};\mathbf{Y}_K|U_K)-I(\mathbf{X};\mathbf{Z}|U_K) = \frac{1}{2}\log\frac{|\tilde{\mathbf{K}}_K+\mathbf{\Sigma}_K|}{|\mathbf{\Sigma}_K|}-\frac{1}{2}\log\frac{|\tilde{\mathbf{K}}_K+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{213}$$

$$I(\mathbf{X};\mathbf{Y}_{K-1}|U_K)-I(\mathbf{X};\mathbf{Z}|U_K) \leq \frac{1}{2}\log\frac{|\tilde{\mathbf{K}}_K+\mathbf{\Sigma}_{K-1}|}{|\mathbf{\Sigma}_{K-1}|}-\frac{1}{2}\log\frac{|\tilde{\mathbf{K}}_K+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{214}$$

Using (213) in (209) yields the desired bound on the $K$th user's secrecy rate as follows

$$R_K \leq \frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_K|}{|\tilde{\mathbf{K}}_K+\mathbf{\Sigma}_K|}-\frac{1}{2}\log\frac{|\mathbf{S}+\mathbf{\Sigma}_Z|}{|\tilde{\mathbf{K}}_K+\mathbf{\Sigma}_Z|} \tag{215}$$

We now bound the $(K-1)$th user's secrecy rate. To this end, first note that

$$\begin{aligned} R_{K-1} &\leq I(U_{K-1};\mathbf{Y}_{K-1}|U_K)-I(U_{K-1};\mathbf{Z}|U_K) && (216)\\ &= I(\mathbf{X};\mathbf{Y}_{K-1}|U_K)-I(\mathbf{X};\mathbf{Z}|U_K)-[I(\mathbf{X};\mathbf{Y}_{K-1}|U_{K-1})-I(\mathbf{X};\mathbf{Z}|U_{K-1})] && (217)\\ &\leq \frac{1}{2}\log\frac{|\tilde{\mathbf{K}}_K+\mathbf{\Sigma}_{K-1}|}{|\mathbf{\Sigma}_{K-1}|}-\frac{1}{2}\log\frac{|\tilde{\mathbf{K}}_K+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|}-[I(\mathbf{X};\mathbf{Y}_{K-1}|U_{K-1})-I(\mathbf{X};\mathbf{Z}|U_{K-1})] && (218) \end{aligned}$$

where in order to obtain (217), we used the Markov chain $U_K\to U_{K-1}\to\mathbf{X}\to(\mathbf{Y}_{K-1},\mathbf{Z})$, and (218) comes from (214). Using the Markov chain $U_K\to U_{K-1}\to\mathbf{X}\to\mathbf{Y}_{K-1}\to\mathbf{Z}$, the mutual information difference in (218) is bounded as

$$\begin{aligned} 0 \leq I(\mathbf{X};\mathbf{Y}_{K-1}|U_{K-1})-I(\mathbf{X};\mathbf{Z}|U_{K-1}) &\leq I(\mathbf{X};\mathbf{Y}_{K-1}|U_K)-I(\mathbf{X};\mathbf{Z}|U_K) && (219)\\ &\leq \frac{1}{2}\log\frac{|\tilde{\mathbf{K}}_K+\mathbf{\Sigma}_{K-1}|}{|\mathbf{\Sigma}_{K-1}|}-\frac{1}{2}\log\frac{|\tilde{\mathbf{K}}_K+\mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} && (220) \end{aligned}$$

Using the analysis carried out in the proof of Theorem 4, we can get a more refined lower bound as follows

$$\begin{aligned} I(\mathbf{X};\mathbf{Y}_{K-1}|U_{K-1})-I(\mathbf{X};\mathbf{Z}|U_{K-1}) \geq{} & \frac{1}{2}\log\frac{|\mathbf{J}(\mathbf{X}+\mathbf{N}_{K-1}|U_{K-1})^{-1}|}{|\mathbf{\Sigma}_{K-1}|}\\ & -\frac{1}{2}\log\frac{|\mathbf{J}(\mathbf{X}+\mathbf{N}_{K-1}|U_{K-1})^{-1}+\mathbf{\Sigma}_Z-\mathbf{\Sigma}_{K-1}|}{|\mathbf{\Sigma}_Z|} \end{aligned} \tag{221}$$

Combining (220) and (221) yields

$$\begin{aligned}
\frac{1}{2}\log\frac{|\mathbf{J}(\mathbf{X}+\mathbf{N}_{K-1}|U_{K-1})^{-1}|}{|\mathbf{J}(\mathbf{X}+\mathbf{N}_{K-1}|U_{K-1})^{-1}+\mathbf{\Sigma}_Z-\mathbf{\Sigma}_{K-1}|}& \\
&\leq I(\mathbf{X};\mathbf{Y}_{K-1}|U_{K-1})-I(\mathbf{X};\mathbf{Z}|U_{K-1})+\frac{1}{2}\log\frac{|\mathbf{\Sigma}_{K-1}|}{|\mathbf{\Sigma}_Z|} \\
&\leq \frac{1}{2}\log\frac{|\tilde{\mathbf{K}}_K+\mathbf{\Sigma}_{K-1}|}{|\tilde{\mathbf{K}}_K+\mathbf{\Sigma}_Z|} \qquad (222)
\end{aligned}$$

Now, using the lower bound on $\tilde{\mathbf{K}}_K$ given in (212), we get

$$\begin{aligned}
\tilde{\mathbf{K}}_K &\succeq \mathbf{J}(\mathbf{X}+\mathbf{N}_K|U_K)^{-1}-\mathbf{\Sigma}_K \qquad (223)\\
&\succeq \mathbf{J}(\mathbf{X}+\mathbf{N}_{K-1}|U_K)^{-1}-\mathbf{\Sigma}_{K-1} \qquad (224)
\end{aligned}$$

where (224) is obtained using Lemma 6. Moreover, since we have $U_K \rightarrow U_{K-1} \rightarrow \mathbf{X}+\mathbf{N}_{K-1}$, the following order exists

$$\mathbf{J}(\mathbf{X}+\mathbf{N}_{K-1}|U_{K-1}) \succeq \mathbf{J}(\mathbf{X}+\mathbf{N}_{K-1}|U_K) \qquad (225)$$

due to Lemma 17. Equation (225) is equivalent to

$$\mathbf{J}(\mathbf{X}+\mathbf{N}_{K-1}|U_{K-1})^{-1} \preceq \mathbf{J}(\mathbf{X}+\mathbf{N}_{K-1}|U_K)^{-1} \qquad (226)$$

using which in (224), we get

$$\tilde{\mathbf{K}}_K \succeq \mathbf{J}(\mathbf{X}+\mathbf{N}_{K-1}|U_{K-1})^{-1}-\mathbf{\Sigma}_{K-1} \qquad (227)$$

We now consider the function

$$r(t)=\frac{1}{2}\log\frac{|\mathbf{A}+\mathbf{B}+t\mathbf{\Delta}|}{|\mathbf{A}+t\mathbf{\Delta}|}, \quad 0\leq t\leq 1 \qquad (228)$$

with the following parameters

$$\begin{aligned}
\mathbf{A} &= \mathbf{J}(\mathbf{X}+\mathbf{N}_{K-1}|U_{K-1})^{-1} \qquad (229)\\
\mathbf{B} &= \mathbf{\Sigma}_Z-\mathbf{\Sigma}_{K-1} \qquad (230)\\
\mathbf{\Delta} &= \tilde{\mathbf{K}}_K+\mathbf{\Sigma}_{K-1}-\mathbf{J}(\mathbf{X}+\mathbf{N}_{K-1}|U_{K-1})^{-1} \qquad (231)
\end{aligned}$$

where $\mathbf{\Delta}\succeq \mathbf{0}$ due to (227). Using this function, we can paraphrase the bound in (222) as

$$-r(0)\leq I(\mathbf{X};\mathbf{Y}_{K-1}|U_{K-1})-I(\mathbf{X};\mathbf{Z}|U_{K-1})+\frac{1}{2}\log\frac{|\mathbf{\Sigma}_{K-1}|}{|\mathbf{\Sigma}_Z|}\leq -r(1) \qquad (232)$$

As shown in Lemma 10, $r(t)$ is continuous and monotonically decreasing in $t$. Thus, there exists a $t^*$ such that

$$-r(t^*) = I(\mathbf{X}; \mathbf{Y}_{K-1}|U_{K-1}) - I(\mathbf{X}; \mathbf{Z}|U_{K-1}) + \frac{1}{2} \log \frac{|\mathbf{\Sigma}_{K-1}|}{|\mathbf{\Sigma}_Z|} \tag{233}$$

due to the intermediate value theorem. Let $\tilde{\mathbf{K}}_{K-1} = \mathbf{A} + t^* \mathbf{\Delta} - \mathbf{\Sigma}_{K-1}$, then we get

$$I(\mathbf{X}; \mathbf{Y}_{K-1}|U_{K-1}) - I(\mathbf{X}; \mathbf{Z}|U_{K-1}) = \frac{1}{2} \log \frac{|\tilde{\mathbf{K}}_{K-1} + \mathbf{\Sigma}_{K-1}|}{|\mathbf{\Sigma}_{K-1}|} - \frac{1}{2} \log \frac{|\tilde{\mathbf{K}}_{K-1} + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{234}$$

We note that using (234) in (218) yields the desired bound on the $(K-1)$th user's secrecy rate as follows

$$R_{K-1} \leq \frac{1}{2} \log \frac{|\tilde{\mathbf{K}}_K + \mathbf{\Sigma}_{K-1}|}{|\tilde{\mathbf{K}}_{K-1} + \mathbf{\Sigma}_{K-1}|} - \frac{1}{2} \log \frac{|\tilde{\mathbf{K}}_K + \mathbf{\Sigma}_Z|}{|\tilde{\mathbf{K}}_{K-1} + \mathbf{\Sigma}_Z|} \tag{235}$$

Moreover, since $\mathbf{\Delta} \succeq \mathbf{0}$ and $0 \leq t \leq 1$, $\tilde{\mathbf{K}}_{K-1} = \mathbf{A} + t^* \mathbf{\Delta} - \mathbf{\Sigma}_{K-1}$ satisfies the following orderings

$$\mathbf{J}(\mathbf{X} + \mathbf{N}_{K-1}|U_{K-1})^{-1} - \mathbf{\Sigma}_{K-1} \preceq \tilde{\mathbf{K}}_{K-1} \preceq \tilde{\mathbf{K}}_K \tag{236}$$

Furthermore, the lower bound in (236) implies the following order

$$\tilde{\mathbf{K}}_{K-1} \succeq \mathbf{J}(\mathbf{X} + \mathbf{N}|U_{K-1})^{-1} - \mathbf{\Sigma}_N \tag{237}$$

for any Gaussian random vector $\mathbf{N}$ such that $\mathbf{\Sigma}_N \preceq \mathbf{\Sigma}_{K-1}$, and is independent of $U_{K-1}, \mathbf{X}$, which is a consequence of Lemma 6. Using (237), and following the proof of Theorem 4, we can show that

$$I(\mathbf{X}; \mathbf{Y}_{K-2}|U_{K-1}) - I(\mathbf{X}; \mathbf{Z}|U_{K-1}) \leq \frac{1}{2} \log \frac{|\tilde{\mathbf{K}}_{K-1} + \mathbf{\Sigma}_{K-2}|}{|\mathbf{\Sigma}_{K-2}|} - \frac{1}{2} \log \frac{|\tilde{\mathbf{K}}_{K-1} + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{238}$$

Thus, as a recap, we have showed that there exists $\tilde{\mathbf{K}}_{K-1}$ such that

$$\mathbf{J}(\mathbf{X} + \mathbf{N}_{K-1}|U_{K-1})^{-1} - \mathbf{\Sigma}_{K-1} \preceq \tilde{\mathbf{K}}_{K-1} \preceq \tilde{\mathbf{K}}_K \tag{239}$$

and

$$I(\mathbf{X}; \mathbf{Y}_{K-1}|U_{K-1}) - I(\mathbf{X}; \mathbf{Z}|U_{K-1}) = \frac{1}{2} \log \frac{|\tilde{\mathbf{K}}_{K-1} + \mathbf{\Sigma}_{K-1}|}{|\mathbf{\Sigma}_{K-1}|} - \frac{1}{2} \log \frac{|\tilde{\mathbf{K}}_{K-1} + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{240}$$

$$I(\mathbf{X}; \mathbf{Y}_{K-2}|U_{K-1}) - I(\mathbf{X}; \mathbf{Z}|U_{K-1}) \leq \frac{1}{2} \log \frac{|\tilde{\mathbf{K}}_{K-1} + \mathbf{\Sigma}_{K-2}|}{|\mathbf{\Sigma}_{K-2}|} - \frac{1}{2} \log \frac{|\tilde{\mathbf{K}}_{K-1} + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} \tag{241}$$

which are analogous to (212), (213), (214). Thus, proceeding in the same manner, for any selection of the joint distribution $p(u_K)p(u_{K-1}|u_K)\dots p(\mathbf{x}|u_2)$, we can show the existence of matrices $\{\tilde{\mathbf{K}}_k\}_{k=1}^{K+1}$ such that

$$\mathbf{0} = \tilde{\mathbf{K}}_1 \preceq \tilde{\mathbf{K}}_2 \preceq \quad \dots \quad \preceq \tilde{\mathbf{K}}_K \preceq \tilde{\mathbf{K}}_{K+1} = \mathbf{S} \tag{242}$$

and

$$I(\mathbf{X};\mathbf{Y}_k|U_k) - I(\mathbf{X};\mathbf{Z}|U_k) = \frac{1}{2}\log\frac{|\tilde{\mathbf{K}}_k + \mathbf{\Sigma}_k|}{|\mathbf{\Sigma}_k|} - \frac{1}{2}\log\frac{|\tilde{\mathbf{K}}_k + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|}, \quad k = 2,\dots,K \tag{243}$$

$$I(\mathbf{X};\mathbf{Y}_{k-1}|U_k) - I(\mathbf{X};\mathbf{Z}|U_k) \leq \frac{1}{2}\log\frac{|\tilde{\mathbf{K}}_k + \mathbf{\Sigma}_{k-1}|}{|\mathbf{\Sigma}_{k-1}|} - \frac{1}{2}\log\frac{|\tilde{\mathbf{K}}_k + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|}, \quad k = 2,\dots,K+1 \tag{244}$$

where $U_{K+1} = \phi$. We now define $\mathbf{K}_k = \tilde{\mathbf{K}}_{k+1} - \tilde{\mathbf{K}}_k,\ k = 1,\dots,K$, which yields $\tilde{\mathbf{K}}_{k+1} = \sum_{i=1}^{k}\mathbf{K}_i$, and in particular, $\mathbf{S} = \sum_{i=1}^{K}\mathbf{K}_i$. Using these new variables in conjunction with (243) and (244) results in

$$\begin{aligned}
R_k &\leq I(U_k;\mathbf{Y}_k|U_{k+1}) - I(U_k;\mathbf{Z}|U_{k+1}) && (245)\\
&= I(\mathbf{X};\mathbf{Y}_k|U_{k+1}) - I(\mathbf{X};\mathbf{Z}|U_{k+1}) - [I(\mathbf{X};\mathbf{Y}_k|U_k) - I(\mathbf{X};\mathbf{Z}|U_k)] && (246)\\
&\leq \frac{1}{2}\log\frac{\left|\tilde{\mathbf{K}}_{k+1} + \mathbf{\Sigma}_k\right|}{|\mathbf{\Sigma}_k|} - \frac{1}{2}\log\frac{\left|\tilde{\mathbf{K}}_{k+1} + \mathbf{\Sigma}_Z\right|}{|\mathbf{\Sigma}_Z|}\\
&\quad - \frac{1}{2}\log\frac{\left|\tilde{\mathbf{K}}_k + \mathbf{\Sigma}_k\right|}{|\mathbf{\Sigma}_k|} + \frac{1}{2}\log\frac{\left|\tilde{\mathbf{K}}_k + \mathbf{\Sigma}_Z\right|}{|\mathbf{\Sigma}_Z|} && (247)\\
&= \frac{1}{2}\log\frac{\left|\tilde{\mathbf{K}}_{k+1} + \mathbf{\Sigma}_k\right|}{\left|\tilde{\mathbf{K}}_k + \mathbf{\Sigma}_k\right|} - \frac{1}{2}\log\frac{\left|\tilde{\mathbf{K}}_{k+1} + \mathbf{\Sigma}_Z\right|}{\left|\tilde{\mathbf{K}}_k + \mathbf{\Sigma}_Z\right|} && (248)\\
&= \frac{1}{2}\log\frac{\left|\sum_{i=1}^{k}\mathbf{K}_i + \mathbf{\Sigma}_k\right|}{\left|\sum_{i=1}^{k-1}\mathbf{K}_i + \mathbf{\Sigma}_k\right|} - \frac{1}{2}\log\frac{\left|\sum_{i=1}^{k}\mathbf{K}_i + \mathbf{\Sigma}_Z\right|}{\left|\sum_{i=1}^{k-1}\mathbf{K}_i + \mathbf{\Sigma}_Z\right|} && (249)
\end{aligned}$$

for $k = 2,\dots,K$. For $k = 1$, the bound in (244), by setting $k = 2$ in the corresponding expression, yields the desired bound on the first user's secrecy rate

$$\begin{aligned}
R_1 &\leq I(\mathbf{X};\mathbf{Y}_1|U_2) - I(\mathbf{X};\mathbf{Z}|U_2) && (250)\\
&\leq \frac{1}{2}\log\frac{|\mathbf{K}_1 + \mathbf{\Sigma}_1|}{|\mathbf{\Sigma}_1|} - \frac{1}{2}\log\frac{|\mathbf{K}_1 + \mathbf{\Sigma}_Z|}{|\mathbf{\Sigma}_Z|} && (251)
\end{aligned}$$

Since for any selection of the joint distribution $p(u_K)p(u_{K-1}|u_K)\dots p(\mathbf{x}|u_2)$, we can establish the bounds in (249) and (251) with positive semi-definite matrices $\{\mathbf{K}_i\}_{i=1}^{K}$ such that $\mathbf{S} = \sum_{i=1}^{K}\mathbf{K}_i$, the union of these bounds over such matrices would be an outer bound for the secrecy capacity region, completing the converse proof of Theorem 3 for an arbitrary $K$.

# 6 Aligned Gaussian MIMO Multi-receiver Wiretap Channel

We now consider the aligned Gaussian MIMO multi-receiver wiretap channel, and prove its secrecy capacity region. To that end, we basically use our capacity result for the degraded Gaussian MIMO multi-receiver wiretap channel in Section 5 in conjunction with the channel enhancement technique [29]. Due to the presence of an eavesdropper in our channel model, there are some differences between the way we invoke the channel enhancement technique and the way it was used in its original version that appeared in [29]. These differences will be pointed out during our proof.

Given the covariance matrices $\{\mathbf{K}_i\}_{i=1}^K$ such that $\sum_{i=1}^K \mathbf{K}_i \preceq \mathbf{S}$, let us define the following rates,

$$R_k^{\text{DPC}}\left(\pi, \{\mathbf{K}_i\}_{i=1}^K, \{\mathbf{\Sigma}_i\}_{i=1}^K, \mathbf{\Sigma}_Z\right) = \frac{1}{2}\log\frac{\left|\sum_{i=1}^k \mathbf{K}_{\pi(i)} + \mathbf{\Sigma}_{\pi(k)}\right|}{\left|\sum_{i=1}^{k-1} \mathbf{K}_{\pi(i)} + \mathbf{\Sigma}_{\pi(k)}\right|} - \frac{1}{2}\log\frac{\left|\sum_{i=1}^k \mathbf{K}_{\pi(i)} + \mathbf{\Sigma}_Z\right|}{\left|\sum_{i=1}^{k-1} \mathbf{K}_{\pi(i)} + \mathbf{\Sigma}_Z\right|}, \quad k=1,\ldots,K \tag{252}$$

where $\pi(\cdot)$ is a one-to-one permutation on $\{1,\ldots,K\}$. We also note that the subscript of $R_k^{\text{DPC}}\left(\pi, \{\mathbf{K}_i\}_{i=1}^K, \{\mathbf{\Sigma}_i\}_{i=1}^K, \mathbf{\Sigma}_Z\right)$ does not denote the $k$th user, instead it denotes the $(K-k+1)$th user in line to be encoded. Rather, the secrecy rate of the $k$th user is given by

$$R_k = R_{\pi^{-1}(k)}^{\text{DPC}}\left(\pi, \{\mathbf{K}_i\}_{i=1}^K, \{\mathbf{\Sigma}_i\}_{i=1}^K, \mathbf{\Sigma}_Z\right) \tag{253}$$

when dirty-paper coding with stochastic encoding is used with an encoding order of $\pi$. We define the following region:

$$\begin{aligned}&\mathcal{R}^{\text{DPC}}\left(\pi, \mathbf{S}, \{\mathbf{\Sigma}_i\}_{i=1}^K, \mathbf{\Sigma}_Z\right)\\ &= \left\{ (R_1,\ldots,R_K) \;\middle|\; \begin{array}{c} R_k = R_{\pi^{-1}(k)}^{\text{DPC}}\left(\pi, \{\mathbf{K}_i\}_{i=1}^K, \{\mathbf{\Sigma}_i\}_{i=1}^K, \mathbf{\Sigma}_Z\right),\; k=1,\ldots,K, \\ \text{for some } \{\mathbf{K}_i\}_{i=1}^K \text{ such that } \mathbf{K}_i \succeq 0,\; i=1,\ldots,K, \\ \text{and } \sum_{i=1}^K \mathbf{K}_i \preceq \mathbf{S} \end{array} \right\}\end{aligned} \tag{254}$$

The secrecy capacity region of the aligned Gaussian MIMO broadcast channel is given by the following theorem.

**Theorem 6** *The secrecy capacity region of the aligned Gaussian MIMO multi-receiver wire-*

*tap channel is given by the convex closure of the following union*

$$\bigcup_{\pi\in\Pi} \mathcal{R}^{\text{DPC}}\left(\pi, \mathbf{S}, \{\mathbf{\Sigma}_i\}_{i=1}^K, \mathbf{\Sigma}_Z\right) \tag{255}$$

*where* $\Pi$ *is the set of all possible one-to-one permutations on* $\{1, \ldots, K\}$.

We will show the achievability of the secrecy rates in Theorem 6 by extending Marton's achievable scheme for broadcast channels [41] to multi-receiver wiretap channels. For that purpose, we will use Theorem 1 of [42], where the authors provided an achievable region for Gaussian vector broadcast channels using Marton's achievable scheme in [41]. While using this result, we will combine it with a stochastic encoding scheme for secrecy purposes. To provide a converse proof for Theorem 6, we will follow the channel enhancement technique [29]. We will show that for any point on the boundary of the secrecy capacity region, there exists a degraded channel such that its secrecy capacity region includes the secrecy capacity region of the original channel, and furthermore, the boundaries of these two regions intersect at this specific point.

## 6.1 Achievability

To show the achievability of the secrecy rates in Theorem 6, we mostly rely on the derivation of the dirty-paper coding region for the Gaussian MIMO broadcast channel in Theorem 1 of [42]. We employ the achievable scheme in [42] in conjunction with a stochastic encoding scheme due to secrecy concerns. Without loss of generality, we consider the identity permutation, i.e., $\pi(k) = k,\ k = 1, \ldots, K$. Let $(\mathbf{V}_1, \ldots, \mathbf{V}_K)$ be arbitrarily correlated random vectors such that

$$(\mathbf{V}_1, \ldots, \mathbf{V}_K) \rightarrow \mathbf{X} \rightarrow (\mathbf{Y}_1, \ldots, \mathbf{Y}_K, \mathbf{Z}) \tag{256}$$

Using these correlated random vectors, we can construct codebooks $\left\{\mathbf{V}_{k,1}^n(W_k, \tilde{W}_k)\right\}_{k=1}^K$, where $W_k \in \left\{1, \ldots, 2^{nR_k}\right\}$, $\tilde{W}_k \in \left\{1, \ldots, 2^{n\tilde{R}_k}\right\},\ k = 1, \ldots, K$, such that each legitimate receiver can decode the following rates

$$R_k + \tilde{R}_k = \frac{1}{2}\log\frac{\left|\sum_{i=1}^k \mathbf{K}_i + \mathbf{\Sigma}_k\right|}{\left|\sum_{i=1}^{k-1} \mathbf{K}_i + \mathbf{\Sigma}_k\right|}, \quad k = 1, \ldots, K \tag{257}$$

for some positive semi-definite matrices $\{\mathbf{K}_i\}_{i=1}^K$ such that $\sum_{k=1}^K \mathbf{K}_k \preceq \mathbf{S}$ [42]. The messages $\left\{\tilde{W}_k\right\}_{k=1}^K$ do not carry any information, and their sole purpose is to confuse the eavesdropper. In other words, the purpose of these messages is to make the eavesdropper spend its decoding capability on them, preventing the eavesdropper to decode the confidential messages $\{W_k\}_{k=1}^K$. Thus, we need to select the rates of these dummy messages $\left\{\tilde{R}_k\right\}_{k=1}^K$ as

follows

$$\tilde{R}_k = \frac{1}{2}\log\frac{\left|\sum_{i=1}^{k}\mathbf{K}_i + \mathbf{\Sigma}_Z\right|}{\left|\sum_{i=1}^{k-1}\mathbf{K}_i + \mathbf{\Sigma}_Z\right|}, \quad k = 1, \ldots, K \tag{258}$$

To achieve the rates given in (257), $\{\mathbf{V}_k\}_{k=1}^K$ should be taken as jointly Gaussian with appropriate covariance matrices. Moreover, it is sufficient to choose $\mathbf{X}$ as a deterministic function of $\{\mathbf{V}_k\}_{k=1}^K$, and the resulting unconditional distribution of $\mathbf{X}$ is also Gaussian with covariance matrix $\sum_{k=1}^K \mathbf{K}_k$ [42].

To complete the proof, we need to show that the above codebook structure fulfills all of the secrecy constraints in (1). To this end, we take a shortcut, by using the fact that, if a codebook satisfies

$$\lim_{n\to\infty}\frac{1}{n}H(W_1,\ldots,W_K|\mathbf{Z}^n) \geq \sum_{k=1}^K R_k \tag{259}$$

then it also satisfies all of the remaining secrecy constraints in (1) [11]. Thus, we only check (259)

$$\begin{aligned}
&\frac{1}{n}H(W_1,\ldots,W_K|\mathbf{Z}^n) = \frac{1}{n}H(W_1,\ldots,W_K,\mathbf{Z}^n) - \frac{1}{n}H(\mathbf{Z}^n) &(260)\\
&= \frac{1}{n}H(\mathbf{V}_{1,1}^n,\ldots,\mathbf{V}_{K,1}^n,W_1,\ldots,W_K,\mathbf{Z}^n) - \frac{1}{n}H(\mathbf{V}_{1,1}^n,\ldots,\mathbf{V}_{K,1}^n|W_1,\ldots,W_K,\mathbf{Z}^n)\\
&\quad - \frac{1}{n}H(\mathbf{Z}^n) &(261)\\
&= \frac{1}{n}H(\mathbf{V}_{1,1}^n,\ldots,\mathbf{V}_{K,1}^n) + \frac{1}{n}H(W_1,\ldots,W_K,\mathbf{Z}^n|\mathbf{V}_{1,1}^n,\ldots,\mathbf{V}_{K,1}^n)\\
&\quad - \frac{1}{n}H(\mathbf{V}_{1,1}^n,\ldots,\mathbf{V}_{K,1}^n|W_1,\ldots,W_K,\mathbf{Z}^n) - \frac{1}{n}H(\mathbf{Z}^n) &(262)\\
&\geq \frac{1}{n}H(\mathbf{V}_{1,1}^n,\ldots,\mathbf{V}_{K,1}^n) - \frac{1}{n}I(\mathbf{V}_{1,1}^n,\ldots,\mathbf{V}_{K,1}^n;\mathbf{Z}^n) - \frac{1}{n}H(\mathbf{V}_{1,1}^n,\ldots,\mathbf{V}_{K,1}^n|W_1,\ldots,W_K,\mathbf{Z}^n)\\
& &(263)
\end{aligned}$$

We will treat each of the three terms in (263) separately. Since $(\mathbf{V}_{1,1}^n,\ldots,\mathbf{V}_{K,1}^n)$ can take $2^{n\sum_{k=1}^K\left(R_k+\tilde{R}_k\right)}$ values uniformly, for the first term in (263), we have

$$\frac{1}{n}H(\mathbf{V}_{1,1}^n,\ldots,\mathbf{V}_{K,1}^n) = \sum_{k=1}^K R_k + \sum_{k=1}^K \tilde{R}_k \tag{264}$$

The second term in (263) can be bounded as

$$\frac{1}{n} I(\mathbf{V}_{1,1}^n, \ldots, \mathbf{V}_{K,1}^n; \mathbf{Z}^n) \leq I(\mathbf{V}_{1,1}, \ldots, \mathbf{V}_{K,1}; \mathbf{Z}) + \epsilon_n \tag{265}$$

$$\leq I(\mathbf{X}; \mathbf{Z}) + \epsilon_n \tag{266}$$

$$= \frac{1}{2} \log \frac{\left| \sum_{k=1}^K \mathbf{K}_k + \mathbf{\Sigma}_Z \right|}{|\mathbf{\Sigma}_Z|} + \epsilon_n \tag{267}$$

where $\epsilon_n \to 0$ as $n \to \infty$. The first inequality can be shown following Lemma 8 of [1], the second inequality follows from the Markov chain in (256), and the equality in (267) comes from our choice of $\mathbf{X}$, which is Gaussian with covariance matrix $\sum_{k=1}^K \mathbf{K}_k$. We now consider the third term in (263). First, we note that given $(W_1 = w_1, \ldots, W_K = w_K)$, $\left(\mathbf{V}_{1,1}^n, \ldots, \mathbf{V}_{K,1}^n\right)$ can take $2^{n \sum_{k=1}^K \tilde{R}_k}$ values, where $\sum_{k=1}^K \tilde{R}_k$ is given by

$$\sum_{k=1}^K \tilde{R}_k = \frac{1}{2} \log \frac{\left| \sum_{k=1}^K \mathbf{K}_k + \mathbf{\Sigma}_Z \right|}{|\mathbf{\Sigma}_Z|} \tag{268}$$

using our selection in (258). Thus, (268) implies that given $(W_1 = w_1, \ldots, W_K = w_K)$, the eavesdropper can decode $\left(\mathbf{V}_{1,1}^n, \ldots, \mathbf{V}_{K,1}^n\right)$ with vanishingly small probability of error. Hence, using Fano's lemma, we get

$$\frac{1}{n} H(\mathbf{V}_{1,1}^n, \ldots, \mathbf{V}_{K,1}^n | W_1, \ldots, W_K, \mathbf{Z}^n) \leq \frac{1}{n} \left[ 1 + \gamma_n \left( \sum_{k=1}^K \tilde{R}_k \right) \right] \tag{269}$$

where $\gamma_n \to 0$ as $n \to \infty$. Thus, plugging (264), (267) and (269) into (263) yields

$$\lim_{n \to \infty} \frac{1}{n} H(W_1, \ldots, W_K | \mathbf{Z}^n) \geq \sum_{k=1}^K R_k \tag{270}$$

which ensures that the rates

$$R_k = \frac{1}{2} \log \frac{\left| \sum_{i=1}^k \mathbf{K}_i + \mathbf{\Sigma}_k \right|}{\left| \sum_{i=1}^{k-1} \mathbf{K}_i + \mathbf{\Sigma}_k \right|} - \frac{1}{2} \log \frac{\left| \sum_{i=1}^k \mathbf{K}_i + \mathbf{\Sigma}_Z \right|}{\left| \sum_{i=1}^{k-1} \mathbf{K}_i + \mathbf{\Sigma}_Z \right|}, \quad k = 1, \ldots, K \tag{271}$$

can be transmitted in perfect secrecy.

## 6.2 Converse

To show the converse, we consider the maximization of the following expression

$$\sum_{k=1}^{K} \mu_k R_k \tag{272}$$

where $\mu_k \geq 0,\ k = 1, \ldots, K$. We note that the maximum value of (272) traces the boundary of the secrecy capacity region, i.e., its maximum value for any non-negative vector $[\mu_1\ \ldots\ \mu_K]$ will give us a point on the boundary of the secrecy capacity region. Let us define $\pi(\cdot)$ to be a one-to-one permutation on $\{1, \ldots, K\}$ such that

$$0 \leq \mu_{\pi(1)} \leq \ldots \leq \mu_{\pi(K)} \tag{273}$$

Furthermore, let $0 < m \leq K$ of $\{\mu_k\}_{k=1}^K$ be strictly positive, i.e., $\mu_{\pi(1)} = \ldots = \mu_{\pi(K-m)} = 0$, and $\mu_{\pi(K-m+1)} > 0$. We now define another permutation $\pi'(\cdot)$ on the strictly positive elements of $\{\mu_k\}_{k=1}^K$ such that $\pi'(l) = \pi(K - m + l),\ l = 1, \ldots, m$. Then, (272) can be expressed as

$$\sum_{k=1}^{K} \mu_k R_k = \sum_{k=1}^{K} \mu_{\pi(k)} R_{\pi(k)} = \sum_{k=1}^{m} \mu_{\pi'(k)} R_{\pi'(k)} \tag{274}$$

We will show that

$$\begin{aligned} \max \sum_{k=1}^{K} \mu_k R_k &= \max \sum_{k=1}^{m} \mu_{\pi'(k)} R_{\pi'(k)} &(275)\\ &\leq \max \sum_{k=1}^{m} \frac{\mu_{\pi'(k)}}{2} \log \frac{\left|\sum_{i=1}^{k} \mathbf{K}_{\pi'(i)} + \boldsymbol{\Sigma}_{\pi'(k)}\right|}{\left|\sum_{i=1}^{k-1} \mathbf{K}_{\pi'(i)} + \boldsymbol{\Sigma}_{\pi'(k)}\right|} \\ &\qquad - \sum_{k=1}^{m} \frac{\mu_{\pi'(k)}}{2} \log \frac{\left|\sum_{i=1}^{k} \mathbf{K}_{\pi'(i)} + \boldsymbol{\Sigma}_Z\right|}{\left|\sum_{i=1}^{k-1} \mathbf{K}_{\pi'(i)} + \boldsymbol{\Sigma}_Z\right|} &(276) \end{aligned}$$

where the last maximization is over all positive semi-definite matrices $\left\{\mathbf{K}_{\pi'(k)}\right\}_{k=1}^m$ such that $\sum_{k=1}^m \mathbf{K}_{\pi'(k)} \preceq \mathbf{S}$. Since the right hand side of (276) is achievable, if we can show that (276) holds for any non-negative vector $[\mu_1\ \ldots\ \mu_K]$, this will complete the proof of Theorem 6. To simplify the notation, without loss of generality, we assume that $\pi'(k) = k,\ k = 1, \ldots, m$. This assumption is equivalent to the assumption that $0 < \mu_1 \leq \ldots \leq \mu_m$, and $\mu_k = 0,\ k = m + 1, \ldots, K$.

We now investigate the maximization in (276). The objective function in (276) is generally non-convex in the covariance matrices $\left\{\mathbf{K}_{\pi'(k)}\right\}_{k=1}^m$ implying that the KKT conditions for this problem are necessary, but not sufficient. Let us construct the Lagrangian for this

optimization problem

$$L\left(\{\mathbf{M}_i\}_{i=1}^m, \mathbf{M}_Z\right) = \sum_{k=1}^m \mu_k R_k^G + \sum_{k=1}^m \mathrm{tr}(\mathbf{K}_k \mathbf{M}_k) + \mathrm{tr}\left(\left(\mathbf{S} - \sum_{k=1}^m \mathbf{K}_k\right)\mathbf{M}_Z\right) \tag{277}$$

where the Lagrange multipliers $\{\mathbf{M}_i\}_{i=1}^m, \mathbf{M}_Z$ are positive semi-definite matrices, and we defined $\left\{R_k^G\right\}_{k=1}^m$ as follows,

$$R_k^G = \frac{1}{2}\log\frac{\left|\sum_{i=1}^k \mathbf{K}_i + \mathbf{\Sigma}_k\right|}{\left|\sum_{i=1}^{k-1} \mathbf{K}_i + \mathbf{\Sigma}_k\right|} - \frac{1}{2}\log\frac{\left|\sum_{i=1}^k \mathbf{K}_i + \mathbf{\Sigma}_Z\right|}{\left|\sum_{i=1}^{k-1} \mathbf{K}_i + \mathbf{\Sigma}_Z\right|}, \quad k = 1, \ldots, m \tag{278}$$

The gradient of $L\left(\{\mathbf{M}_i\}_{i=1}^m, \mathbf{M}_Z\right)$ with respect to $\mathbf{K}_j$ for any $j = 1, \ldots, m-1$, is given by

$$\begin{aligned}\nabla_{\mathbf{K}_j} L\left(\{\mathbf{M}_i\}_{i=1}^m, \mathbf{M}_Z\right) = &\sum_{k=j}^m \frac{\mu_k}{2}\left(\sum_{i=1}^k \mathbf{K}_i + \mathbf{\Sigma}_k\right)^{-1} - \sum_{k=j+1}^m \frac{\mu_k}{2}\left(\sum_{i=1}^{k-1} \mathbf{K}_i + \mathbf{\Sigma}_k\right)^{-1} \\ &- \sum_{k=j}^m \frac{\mu_k}{2}\left(\sum_{i=1}^k \mathbf{K}_i + \mathbf{\Sigma}_Z\right)^{-1} + \sum_{k=j+1}^m \frac{\mu_k}{2}\left(\sum_{i=1}^{k-1} \mathbf{K}_i + \mathbf{\Sigma}_Z\right)^{-1} \\ &+ \mathbf{M}_j - \mathbf{M}_Z \end{aligned} \tag{279}$$

and the gradient of $L\left(\{\mathbf{M}_i\}_{i=1}^m, \mathbf{M}_Z\right)$ with respect to $\mathbf{K}_m$ is given by

$$\nabla_{\mathbf{K}_m} L\left(\{\mathbf{M}_i\}_{i=1}^m, \mathbf{M}_Z\right) = \frac{\mu_m}{2}\left(\sum_{i=1}^m \mathbf{K}_i + \mathbf{\Sigma}_m\right)^{-1} - \frac{\mu_m}{2}\left(\sum_{i=1}^m \mathbf{K}_i + \mathbf{\Sigma}_Z\right)^{-1} + \mathbf{M}_m - \mathbf{M}_Z \tag{280}$$

The KKT conditions are given by

$$\nabla_{\mathbf{K}_j} L\left(\{\mathbf{M}_i\}_{i=1}^m, \mathbf{M}_Z\right) = \mathbf{0}, \quad j = 1, \ldots, m \tag{281}$$

$$\mathrm{tr}(\mathbf{K}_j \mathbf{M}_j) = 0, \quad j = 1, \ldots, m \tag{282}$$

$$\mathrm{tr}\left(\left(\mathbf{S} - \sum_{k=1}^m \mathbf{K}_k\right)\mathbf{M}_Z\right) = 0 \tag{283}$$

We note that since $\mathrm{tr}(\mathbf{K}_j \mathbf{M}_j) = \mathrm{tr}(\mathbf{M}_j \mathbf{K}_j)$, and $\mathbf{M}_j \succeq \mathbf{0}, \mathbf{K}_j \succeq \mathbf{0}$, we have $\mathbf{M}_j \mathbf{K}_j = \mathbf{K}_j \mathbf{M}_j = \mathbf{0}$. Thus, the KKT conditions in (282) are equivalent to

$$\mathbf{M}_j \mathbf{K}_j = \mathbf{K}_j \mathbf{M}_j = \mathbf{0}, \quad j = 1, \ldots, m \tag{284}$$

Similarly, we also have

$$\mathbf{M}_Z\left(\mathbf{S}-\sum_{k=1}^{m}\mathbf{K}_k\right)=\left(\mathbf{S}-\sum_{k=1}^{m}\mathbf{K}_k\right)\mathbf{M}_Z=\mathbf{0} \tag{285}$$

Subtracting the gradient of the Lagrangian with respect to $\mathbf{K}_{j+1}$ from the one with respect to $\mathbf{K}_j$, for $j=1,\ldots,m-1$, we get

$$\begin{aligned}
&\nabla_{\mathbf{K}_j}L\left(\{\mathbf{M}_i\}_{i=1}^{m},\mathbf{M}_Z\right)-\nabla_{\mathbf{K}_{j+1}}L\left(\{\mathbf{M}_i\}_{i=1}^{m},\mathbf{M}_Z\right)\\
&=\sum_{k=j}^{m}\frac{\mu_k}{2}\left(\sum_{i=1}^{k}\mathbf{K}_i+\mathbf{\Sigma}_k\right)^{-1}-\sum_{k=j+1}^{m}\frac{\mu_k}{2}\left(\sum_{i=1}^{k-1}\mathbf{K}_i+\mathbf{\Sigma}_k\right)^{-1}\\
&\quad-\sum_{k=j}^{m}\frac{\mu_k}{2}\left(\sum_{i=1}^{k}\mathbf{K}_i+\mathbf{\Sigma}_Z\right)^{-1}+\sum_{k=j+1}^{m}\frac{\mu_k}{2}\left(\sum_{i=1}^{k-1}\mathbf{K}_i+\mathbf{\Sigma}_Z\right)^{-1}+\mathbf{M}_j-\mathbf{M}_Z\\
&\quad-\sum_{k=j+1}^{m}\frac{\mu_k}{2}\left(\sum_{i=1}^{k}\mathbf{K}_i+\mathbf{\Sigma}_k\right)^{-1}+\sum_{k=j+2}^{m}\frac{\mu_k}{2}\left(\sum_{i=1}^{k-1}\mathbf{K}_i+\mathbf{\Sigma}_k\right)^{-1}\\
&\quad+\sum_{k=j+1}^{m}\frac{\mu_k}{2}\left(\sum_{i=1}^{k}\mathbf{K}_i+\mathbf{\Sigma}_Z\right)^{-1}-\sum_{k=j+2}^{m}\frac{\mu_k}{2}\left(\sum_{i=1}^{k-1}\mathbf{K}_i+\mathbf{\Sigma}_Z\right)^{-1}-\mathbf{M}_{j+1}+\mathbf{M}_Z \qquad (286)\\
&=\frac{\mu_j}{2}\left(\sum_{i=1}^{j}\mathbf{K}_i+\mathbf{\Sigma}_j\right)^{-1}-\frac{\mu_{j+1}}{2}\left(\sum_{i=1}^{j}\mathbf{K}_i+\mathbf{\Sigma}_{j+1}\right)^{-1}\\
&\quad-\frac{\mu_j}{2}\left(\sum_{i=1}^{j}\mathbf{K}_i+\mathbf{\Sigma}_Z\right)^{-1}+\frac{\mu_{j+1}}{2}\left(\sum_{i=1}^{j}\mathbf{K}_i+\mathbf{\Sigma}_Z\right)^{-1}+\mathbf{M}_j-\mathbf{M}_{j+1} \qquad (287)
\end{aligned}$$

Thus, using (284), (285), (287), we can express the KKT conditions in (281), (282), (283) as follows

$$\begin{aligned}
\mu_j\left(\sum_{i=1}^{j}\mathbf{K}_i+\mathbf{\Sigma}_j\right)^{-1}+(\mu_{j+1}-\mu_j)\left(\sum_{i=1}^{j}\mathbf{K}_i+\mathbf{\Sigma}_Z\right)^{-1}+\mathbf{M}_j=\mu_{j+1}\left(\sum_{i=1}^{j}\mathbf{K}_i+\mathbf{\Sigma}_{j+1}\right)^{-1}\\
+\mathbf{M}_{j+1},\quad j=1,\ldots,m-1
\end{aligned} \tag{288}$$

$$\mu_m\left(\sum_{i=1}^{m}\mathbf{K}_i+\mathbf{\Sigma}_m\right)^{-1}+\mathbf{M}_m=\mu_m\left(\sum_{i=1}^{m}\mathbf{K}_i+\mathbf{\Sigma}_Z\right)^{-1}+\mathbf{M}_Z \tag{289}$$

$$\mathbf{K}_j\mathbf{M}_j=\mathbf{M}_j\mathbf{K}_j=\mathbf{0},\quad j=1,\ldots,m \tag{290}$$

$$\mathbf{M}_Z\left(\mathbf{S}-\sum_{k=1}^{m}\mathbf{K}_k\right)=\left(\mathbf{S}-\sum_{k=1}^{m}\mathbf{K}_k\right)\mathbf{M}_Z=\mathbf{0} \tag{291}$$

where we also embed the multiplications by 2 into the Lagrange multipliers.

We now present a lemma which will be instrumental in constructing a degraded Gaussian MIMO multi-receiver wiretap channel, such that the secrecy capacity region of the constructed channel includes the secrecy capacity region of the original channel, and the boundary of the secrecy capacity region of this constructed channel coincides with the boundary of the secrecy capacity region of the original channel at a certain point for a given non-negative vector $[\mu_1 \ \dots \ \mu_K]$.

**Lemma 18** *Given the covariance matrices $\{\mathbf{K}_j\}_{j=1}^m$ satisfying the KKT conditions given in (288)-(291), there exist noise covariance matrices $\{\tilde{\mathbf{\Sigma}}_j\}_{j=1}^m$ such that*

1. $\tilde{\mathbf{\Sigma}}_j \preceq \mathbf{\Sigma}_j, \ j = 1, \dots, m.$
2. $\mathbf{0} \prec \tilde{\mathbf{\Sigma}}_1 \preceq \dots \preceq \tilde{\mathbf{\Sigma}}_m \preceq \mathbf{\Sigma}_Z$
3. $\mu_j \left(\sum_{i=1}^j \mathbf{K}_i + \tilde{\mathbf{\Sigma}}_j\right)^{-1} + (\mu_{j+1} - \mu_j) \left(\sum_{i=1}^j \mathbf{K}_i + \mathbf{\Sigma}_Z\right)^{-1} = \mu_{j+1} \left(\sum_{i=1}^j \mathbf{K}_i + \tilde{\mathbf{\Sigma}}_{j+1}\right)^{-1},$

   *for* $j = 1, \dots, m-1,$ *and*

   $\mu_m \left(\sum_{i=1}^m \mathbf{K}_i + \tilde{\mathbf{\Sigma}}_m\right)^{-1} = \mu_m \big(\sum_{i=1}^m \mathbf{K}_i + \mathbf{\Sigma}_Z\big)^{-1} + \mathbf{M}_Z$
4. $\left(\sum_{i=1}^j \mathbf{K}_i + \tilde{\mathbf{\Sigma}}_j\right)^{-1} \left(\sum_{i=1}^{j-1} \mathbf{K}_i + \tilde{\mathbf{\Sigma}}_j\right) = \left(\sum_{i=1}^j \mathbf{K}_i + \mathbf{\Sigma}_j\right)^{-1} \left(\sum_{i=1}^{j-1} \mathbf{K}_i + \mathbf{\Sigma}_j\right)$

   *for* $j = 1, \dots, m$
5. $\left(\mathbf{S} + \tilde{\mathbf{\Sigma}}_m\right) \left(\sum_{i=1}^m \mathbf{K}_i + \tilde{\mathbf{\Sigma}}_m\right)^{-1} = (\mathbf{S} + \mathbf{\Sigma}_Z) \left(\sum_{i=1}^m \mathbf{K}_i + \mathbf{\Sigma}_Z\right)^{-1}$

The proof of this lemma is given in Appendix F.

Without loss of generality, we have already fixed $[\mu_1 \ \dots \ \mu_K]$ such that $0 < \mu_1 \leq \dots \leq \mu_m$, and $\mu_k = 0, \ k = m+1, \dots, K$ for some $0 < m \leq K$. For this fixed $[\mu_1 \ \dots \ \mu_K]$, assume that $\{\mathbf{K}_k^*\}_{k=1}^m$ achieves the maximum of (276). Since these covariance matrices need to satisfy the KKT conditions given in (288)-(291), Lemma 18 ensures the existence of the covariance matrices $\{\tilde{\mathbf{\Sigma}}_j\}_{j=1}^m$ that have the properties listed in Lemma 18. Thus, we can define a degraded Gaussian MIMO multi-receiver wiretap channel that has the following noise covariance matrices

$$\hat{\mathbf{\Sigma}}_k = \begin{cases} \tilde{\mathbf{\Sigma}}_k, & 1 \leq k \leq m \\ \alpha_{k-m} \tilde{\mathbf{\Sigma}}_1, & m+1 \leq k \leq K \end{cases} \tag{292}$$

where $0 < \alpha_{k-m} \leq 1$ are chosen to satisfy $\alpha_{k-m}\tilde{\mathbf{\Sigma}}_1 \preceq \mathbf{\Sigma}_k$ for $k = m+1, \dots, K$, where the existence of such $\{\alpha_{k-m}\}_{k=m+1}^K$ are ensured by the positive definiteness of $\{\mathbf{\Sigma}_k\}_{k=1}^K$. The noise covariance matrix of the eavesdropper is the same as in the original channel, i.e., $\mathbf{\Sigma}_Z$. Since this channel is degraded, its secrecy capacity region is given by Theorem 3. Moreover, since $\hat{\mathbf{\Sigma}}_k \preceq \mathbf{\Sigma}_k, \ k = 1, \dots, K$, and the noise covariance matrices in the constructed degraded

channel and the original channel are the same, the secrecy capacity region of this degraded channel outer bounds that of the original channel. Next, we show that for the so-far fixed $[\mu_1 \ \dots \ \mu_K]$, the boundaries of these two regions intersect at this point. For this purpose, reconsider the maximization problem in (272)

$$\max \sum_{k=1}^{K} \mu_k R_k = \max \sum_{k=1}^{m} \mu_k R_k \tag{293}$$

$$\leq \max_{\substack{\mathbf{K}_i \succeq 0,\ i=1,\dots,K \\ \sum_{i=1}^{K} \mathbf{K}_i \preceq \mathbf{S}}} \sum_{k=1}^{m} \frac{\mu_k}{2} \left[ \log \frac{\left|\sum_{i=1}^{k} \mathbf{K}_i + \sum_{i=m+1}^{K} \mathbf{K}_i + \tilde{\mathbf{\Sigma}}_k\right|}{\left|\sum_{i=1}^{k-1} \mathbf{K}_i + \sum_{i=m+1}^{K} \mathbf{K}_i + \tilde{\mathbf{\Sigma}}_k\right|} - \log \frac{\left|\sum_{i=1}^{k} \mathbf{K}_i + \sum_{i=m+1}^{K} \mathbf{K}_i + \mathbf{\Sigma}_Z\right|}{\left|\sum_{i=1}^{k-1} \mathbf{K}_i + \sum_{i=m+1}^{K} \mathbf{K}_i + \mathbf{\Sigma}_Z\right|} \right] \tag{294}$$

$$= \max_{\substack{\mathbf{K}_i \succeq 0,\ i=1,\dots,m \\ \sum_{i=1}^{m} \mathbf{K}_i \preceq \mathbf{S}}} \sum_{k=1}^{m} \frac{\mu_k}{2} \left[ \log \frac{\left|\sum_{i=1}^{k} \mathbf{K}_i + \tilde{\mathbf{\Sigma}}_k\right|}{\left|\sum_{i=1}^{k-1} \mathbf{K}_i + \tilde{\mathbf{\Sigma}}_k\right|} - \log \frac{\left|\sum_{i=1}^{k} \mathbf{K}_i + \mathbf{\Sigma}_Z\right|}{\left|\sum_{i=1}^{k-1} \mathbf{K}_i + \mathbf{\Sigma}_Z\right|} \right] \tag{295}$$

where (293) is implied by the fact that for the fixed $[\mu_1 \ \dots \ \mu_K]$, we assumed that $\mu_k = 0,\ k = m+1, \dots, K$ and $0 < \mu_1 \leq \dots \leq \mu_m$, (294) follows from the facts that the constructed degraded channel includes the secrecy capacity region of the original channel, and the secrecy capacity region of the degraded channel is given by Theorem 3. The last equation, i.e., (295), comes from the fact that, since $\mu_k = 0,\ k = m+1, \dots, K$, there is no loss of optimality in choosing $\mathbf{K}_k = \mathbf{0},\ k = m+1, \dots, K$. We now claim that the maximum in (295) is achieved by $\{\mathbf{K}_k^*\}_{k=1}^m$. To prove this claim, we first define

$$R_k^* = \frac{1}{2} \log \frac{\left|\sum_{i=1}^{k} \mathbf{K}_i^* + \tilde{\mathbf{\Sigma}}_k\right|}{\left|\sum_{i=1}^{k-1} \mathbf{K}_i^* + \tilde{\mathbf{\Sigma}}_k\right|} - \frac{1}{2} \log \frac{\left|\sum_{i=1}^{k} \mathbf{K}_i^* + \mathbf{\Sigma}_Z\right|}{\left|\sum_{i=1}^{k-1} \mathbf{K}_i^* + \mathbf{\Sigma}_Z\right|}, \quad k = 1, \dots, m \tag{296}$$

and

$$\hat{R}_k = \frac{1}{2} \log \frac{\left|\sum_{i=1}^{k} \mathbf{K}_i + \tilde{\mathbf{\Sigma}}_k\right|}{\left|\sum_{i=1}^{k-1} \mathbf{K}_i + \tilde{\mathbf{\Sigma}}_k\right|} - \frac{1}{2} \log \frac{\left|\sum_{i=1}^{k} \mathbf{K}_i + \mathbf{\Sigma}_Z\right|}{\left|\sum_{i=1}^{k-1} \mathbf{K}_i + \mathbf{\Sigma}_Z\right|}, \quad k = 1, \dots, m \tag{297}$$

for some arbitrary positive semi-definite matrices $\{\mathbf{K}_i\}_{i=1}^m$ such that $\sum_{i=1}^m \mathbf{K}_i \preceq \mathbf{S}$. To prove that the maximum in (295) is achieved by $\{\mathbf{K}_k^*\}_{k=1}^m$, we will show that

$$\sum_{k=1}^{m} \mu_k R_k^* - \sum_{k=1}^{m} \mu_k \hat{R}_k \geq 0 \tag{298}$$

To this end, consider the first summation in (298)

$$\begin{aligned}
\sum_{k=1}^{m}\mu_k R_k^* &= \sum_{k=1}^{m}\frac{\mu_k}{2}\left(\log\left|\sum_{i=1}^{k}\mathbf{K}_i^*+\tilde{\mathbf{\Sigma}}_k\right|-\log\left|\sum_{i=1}^{k}\mathbf{K}_i^*+\mathbf{\Sigma}_Z\right|\right)\\
&\quad-\sum_{k=2}^{m}\frac{\mu_k}{2}\left(\log\left|\sum_{i=1}^{k-1}\mathbf{K}_i^*+\tilde{\mathbf{\Sigma}}_k\right|-\log\left|\sum_{i=1}^{k-1}\mathbf{K}_i^*+\mathbf{\Sigma}_Z\right|\right)\\
&\quad-\frac{\mu_1}{2}\log\frac{\left|\tilde{\mathbf{\Sigma}}_1\right|}{|\mathbf{\Sigma}_Z|} &(299)\\
&= \sum_{k=1}^{m}\frac{\mu_k}{2}\left(\log\left|\sum_{i=1}^{k}\mathbf{K}_i^*+\tilde{\mathbf{\Sigma}}_k\right|-\log\left|\sum_{i=1}^{k}\mathbf{K}_i^*+\mathbf{\Sigma}_Z\right|\right)\\
&\quad-\sum_{k=1}^{m-1}\frac{\mu_{k+1}}{2}\left(\log\left|\sum_{i=1}^{k}\mathbf{K}_i^*+\tilde{\mathbf{\Sigma}}_{k+1}\right|-\log\left|\sum_{i=1}^{k}\mathbf{K}_i^*+\mathbf{\Sigma}_Z\right|\right)\\
&\quad-\frac{\mu_1}{2}\log\frac{\left|\tilde{\mathbf{\Sigma}}_1\right|}{|\mathbf{\Sigma}_Z|} &(300)\\
&= \frac{\mu_m}{2}\log\frac{\left|\sum_{i=1}^{m}\mathbf{K}_i^*+\tilde{\mathbf{\Sigma}}_m\right|}{\left|\sum_{i=1}^{m}\mathbf{K}_i^*+\mathbf{\Sigma}_Z\right|}\\
&\quad+\sum_{k=1}^{m-1}\frac{\mu_k}{2}\left(\log\left|\sum_{i=1}^{k}\mathbf{K}_i^*+\tilde{\mathbf{\Sigma}}_k\right|-\log\left|\sum_{i=1}^{k}\mathbf{K}_i^*+\mathbf{\Sigma}_Z\right|\right)\\
&\quad-\sum_{k=1}^{m-1}\frac{\mu_{k+1}}{2}\left(\log\left|\sum_{i=1}^{k}\mathbf{K}_i^*+\tilde{\mathbf{\Sigma}}_{k+1}\right|-\log\left|\sum_{i=1}^{k}\mathbf{K}_i^*+\mathbf{\Sigma}_Z\right|\right)\\
&\quad-\frac{\mu_1}{2}\log\frac{\left|\tilde{\mathbf{\Sigma}}_1\right|}{|\mathbf{\Sigma}_Z|} &(301)\\
&= \frac{\mu_m}{2}\log\frac{\left|\sum_{i=1}^{m}\mathbf{K}_i^*+\tilde{\mathbf{\Sigma}}_m\right|}{\left|\sum_{i=1}^{m}\mathbf{K}_i^*+\mathbf{\Sigma}_Z\right|}+\sum_{k=1}^{m-1}\frac{\mu_k}{2}\log\left|\sum_{i=1}^{k}\mathbf{K}_i^*+\tilde{\mathbf{\Sigma}}_k\right|\\
&\quad+\sum_{k=1}^{m-1}\frac{\mu_{k+1}-\mu_k}{2}\log\left|\sum_{i=1}^{k}\mathbf{K}_i^*+\mathbf{\Sigma}_Z\right|-\sum_{k=1}^{m-1}\frac{\mu_{k+1}}{2}\log\left|\sum_{i=1}^{k}\mathbf{K}_i^*+\tilde{\mathbf{\Sigma}}_{k+1}\right|\\
&\quad-\frac{\mu_1}{2}\log\frac{\left|\tilde{\mathbf{\Sigma}}_1\right|}{|\mathbf{\Sigma}_Z|} &(302)
\end{aligned}$$

Similarly, we have

$$\sum_{k=1}^{m} \mu_k \hat{R}_k = \frac{\mu_m}{2} \log \frac{\left|\sum_{i=1}^{m} \mathbf{K}_i + \tilde{\mathbf{\Sigma}}_m\right|}{\left|\sum_{i=1}^{m} \mathbf{K}_i + \mathbf{\Sigma}_Z\right|} + \sum_{k=1}^{m-1} \frac{\mu_k}{2} \log \left|\sum_{i=1}^{k} \mathbf{K}_i + \tilde{\mathbf{\Sigma}}_k\right|$$
$$+ \sum_{k=1}^{m-1} \frac{\mu_{k+1} - \mu_k}{2} \log \left|\sum_{i=1}^{k} \mathbf{K}_i + \mathbf{\Sigma}_Z\right| - \sum_{k=1}^{m-1} \frac{\mu_{k+1}}{2} \log \left|\sum_{i=1}^{k} \mathbf{K}_i + \tilde{\mathbf{\Sigma}}_{k+1}\right|$$
$$- \frac{\mu_1}{2} \log \frac{\left|\tilde{\mathbf{\Sigma}}_1\right|}{\left|\mathbf{\Sigma}_Z\right|} \tag{303}$$

We define the following matrices

$$\mathbf{\Delta}_k = \sum_{i=1}^{k} \mathbf{K}_i - \sum_{i=1}^{k} \mathbf{K}_i^*, \quad k = 1, \ldots, m \tag{304}$$

Using (302), (303) and (304), the difference in (298) can be expressed as

$$\sum_{k=1}^{m} \mu_k R_k^* - \sum_{k=1}^{m} \mu_k \hat{R}_k = \frac{\mu_m}{2} \log \frac{\left|\sum_{i=1}^{m} \mathbf{K}_i^* + \tilde{\mathbf{\Sigma}}_m\right|}{\left|\sum_{i=1}^{m} \mathbf{K}_i^* + \mathbf{\Sigma}_Z\right|} - \frac{\mu_m}{2} \log \frac{\left|\sum_{i=1}^{m} \mathbf{K}_i + \tilde{\mathbf{\Sigma}}_m\right|}{\left|\sum_{i=1}^{m} \mathbf{K}_i + \mathbf{\Sigma}_Z\right|}$$
$$- \sum_{k=1}^{m-1} \frac{\mu_k}{2} \log \left|\mathbf{I} + \left(\sum_{i=1}^{k} \mathbf{K}_i^* + \tilde{\mathbf{\Sigma}}_k\right)^{-1} \mathbf{\Delta}_k\right|$$
$$- \sum_{k=1}^{m-1} \frac{\mu_{k+1} - \mu_k}{2} \log \left|\mathbf{I} + \left(\sum_{i=1}^{k} \mathbf{K}_i^* + \mathbf{\Sigma}_Z\right)^{-1} \mathbf{\Delta}_k\right|$$
$$+ \sum_{k=1}^{m-1} \frac{\mu_{k+1}}{2} \log \left|\mathbf{I} + \left(\sum_{i=1}^{k} \mathbf{K}_i^* + \tilde{\mathbf{\Sigma}}_{k+1}\right)^{-1} \mathbf{\Delta}_k\right| \tag{305}$$

We first note that

$$\frac{\left|\sum_{i=1}^{m} \mathbf{K}_i^* + \tilde{\mathbf{\Sigma}}_m\right|}{\left|\sum_{i=1}^{m} \mathbf{K}_i^* + \mathbf{\Sigma}_Z\right|} = \frac{\left|\mathbf{S} + \tilde{\mathbf{\Sigma}}_m\right|}{\left|\mathbf{S} + \mathbf{\Sigma}_Z\right|} \geq \frac{\left|\sum_{i=1}^{m} \mathbf{K}_i + \tilde{\mathbf{\Sigma}}_m\right|}{\left|\sum_{i=1}^{m} \mathbf{K}_i + \mathbf{\Sigma}_Z\right|} \tag{306}$$

where the equality is due to the fifth part of Lemma 18, and the inequality follows from the fact that the function

$$\frac{\left|\mathbf{A} + \tilde{\mathbf{\Sigma}}_m\right|}{\left|\mathbf{A} + \mathbf{\Sigma}_Z\right|} \tag{307}$$

is monotonically increasing in the positive semi-definite matrix $\mathbf{A}$ as can be deduced from

(100), and that $\sum_{i=1}^m \mathbf{K}_i \preceq \mathbf{S}$. Furthermore, we have

$$\frac{\mu_k}{\mu_{k+1}} \log\left|\mathbf{I} + \left(\sum_{i=1}^k \mathbf{K}_i^* + \tilde{\mathbf{\Sigma}}_k\right)^{-1} \mathbf{\Delta}_k\right| + \frac{\mu_{k+1}-\mu_k}{\mu_{k+1}} \log\left|\mathbf{I} + \left(\sum_{i=1}^k \mathbf{K}_i^* + \mathbf{\Sigma}_Z\right)^{-1} \mathbf{\Delta}_k\right|$$

$$\leq \log\left|\mathbf{I} + \frac{\mu_k}{\mu_{k+1}}\left(\sum_{i=1}^k \mathbf{K}_i^* + \tilde{\mathbf{\Sigma}}_k\right)^{-1} \mathbf{\Delta}_k + \frac{\mu_{k+1}-\mu_k}{\mu_{k+1}}\left(\sum_{i=1}^k \mathbf{K}_i^* + \mathbf{\Sigma}_Z\right)^{-1} \mathbf{\Delta}_k\right| \tag{308}$$

$$= \log\left|\mathbf{I} + \left(\sum_{i=1}^k \mathbf{K}_i^* + \tilde{\mathbf{\Sigma}}_{k+1}\right)^{-1} \mathbf{\Delta}_k\right| \tag{309}$$

where the inequality in (308) follows from the concavity of $\log|\cdot|$ in positive semi-definite matrices, and (309) follows from the third part of Lemma 18. Using (306) and (309) in (305) yields

$$\sum_{k=1}^m \mu_k R_k^* - \sum_{k=1}^m \mu_k \hat{R}_k \geq 0 \tag{310}$$

which implies that the maximum in (295) is achieved by $\{\mathbf{K}_k^*\}_{k=1}^m$. Thus, using this fact in (295), we get

$$\max \sum_{k=1}^K \mu_k R_k \leq \sum_{k=1}^m \frac{\mu_k}{2}\left[\log\frac{\left|\sum_{i=1}^k \mathbf{K}_i^* + \tilde{\mathbf{\Sigma}}_k\right|}{\left|\sum_{i=1}^{k-1} \mathbf{K}_i^* + \tilde{\mathbf{\Sigma}}_k\right|} - \log\frac{\left|\sum_{i=1}^k \mathbf{K}_i^* + \mathbf{\Sigma}_Z\right|}{\left|\sum_{i=1}^{k-1} \mathbf{K}_i^* + \mathbf{\Sigma}_Z\right|}\right] \tag{311}$$

$$= \sum_{k=1}^m \frac{\mu_k}{2}\left[\log\frac{\left|\sum_{i=1}^k \mathbf{K}_i^* + \mathbf{\Sigma}_k\right|}{\left|\sum_{i=1}^{k-1} \mathbf{K}_i^* + \mathbf{\Sigma}_k\right|} - \log\frac{\left|\sum_{i=1}^k \mathbf{K}_i^* + \mathbf{\Sigma}_Z\right|}{\left|\sum_{i=1}^{k-1} \mathbf{K}_i^* + \mathbf{\Sigma}_Z\right|}\right] \tag{312}$$

where the equality follows from the fourth part of Lemma 18. Since the right hand side of (312) is achievable, and we can get a similar outer bound for any non-negative vector $[\mu_1 \ \ldots \ \mu_K]$, this completes the converse proof for the aligned Gaussian MIMO channel.

# 7 General Gaussian MIMO Multi-receiver Wiretap Channel

In this final part of the paper, we consider the general Gaussian multi-receiver wiretap channel and prove its secrecy capacity region. The main idea in this section is to construct an aligned channel that is indexed by a scalar variable, and then show that this aligned channel has the same secrecy capacity region as the original channel in the limit of this indexing parameter on the constructed aligned channel. This argument was previously used in [29, 30]. The way we use this argument here is different from [29] because there are no

secrecy constraints in [29], and it is different from [30] because there are multiple legitimate receivers here.

Given the covariance matrices $\{\mathbf{K}_k\}_{k=1}^K$ such that $\sum_{k=1}^K \mathbf{K}_k \preceq \mathbf{S}$, we define the following rates

$$\begin{aligned}&R_k^{\text{DPC}}\left(\pi, \{\mathbf{K}_i\}_{i=1}^K, \{\mathbf{\Sigma}_i\}_{i=1}^K, \mathbf{\Sigma}_Z, \{\mathbf{H}_i\}_{i=1}^K, \mathbf{H}_Z\right)\\ &= \frac{1}{2}\log\frac{\left|\mathbf{H}_{\pi(k)}\left(\sum_{i=1}^k \mathbf{K}_{\pi(i)}\right)\mathbf{H}_{\pi(k)}^\top + \mathbf{\Sigma}_{\pi(k)}\right|}{\left|\mathbf{H}_{\pi(k)}\left(\sum_{i=1}^{k-1} \mathbf{K}_{\pi(i)}\right)\mathbf{H}_{\pi(k)}^\top + \mathbf{\Sigma}_{\pi(k)}\right|} - \frac{1}{2}\log\frac{\left|\mathbf{H}_Z\left(\sum_{i=1}^k \mathbf{K}_{\pi(i)}\right)\mathbf{H}_Z^\top + \mathbf{\Sigma}_Z\right|}{\left|\mathbf{H}_Z\left(\sum_{i=1}^{k-1} \mathbf{K}_{\pi(i)}\right)\mathbf{H}_Z^\top + \mathbf{\Sigma}_Z\right|},\\ &\qquad k = 1, \ldots, K \end{aligned} \tag{313}$$

where $\pi(\cdot)$ is a one-to-one permutation on $\{1, \ldots, K\}$. We also note that the subscript of $R_k^{\text{DPC}}\left(\pi, \{\mathbf{K}_i\}_{i=1}^K, \{\mathbf{\Sigma}_i\}_{i=1}^K, \mathbf{\Sigma}_Z, \{\mathbf{H}_i\}_{i=1}^K, \mathbf{H}_Z\right)$ does not denote the $k$th user, instead it denotes the $(K-k+1)$th user in line to be encoded. Rather, the secrecy rate of the $k$th user is given by

$$R_k = R_{\pi^{-1}(k)}^{\text{DPC}}\left(\pi, \{\mathbf{K}_i\}_{i=1}^K, \{\mathbf{\Sigma}_i\}_{i=1}^K, \mathbf{\Sigma}_Z, \{\mathbf{H}_i\}_{i=1}^K, \mathbf{H}_Z\right) \tag{314}$$

when dirty-paper coding with stochastic encoding is used with an encoding order of $\pi$.

We define the following region.

$$\begin{aligned}&\mathcal{R}^{\text{DPC}}\left(\pi, \mathbf{S}, \{\mathbf{\Sigma}_i\}_{i=1}^K, \mathbf{\Sigma}_Z, \{\mathbf{H}_i\}_{i=1}^K, \mathbf{H}_Z\right)\\ &= \left\{ (R_1, \ldots, R_K) \;\middle|\; \begin{array}{c} R_k = R_{\pi^{-1}(k)}^{\text{DPC}}\left(\pi, \{\mathbf{K}_i\}_{i=1}^K, \{\mathbf{\Sigma}_i\}_{i=1}^K, \mathbf{\Sigma}_Z, \{\mathbf{H}_i\}_{i=1}^K, \mathbf{H}_Z\right), \\ k = 1, \ldots, K, \text{ for some } \{\mathbf{K}_i\}_{i=1}^K \text{ such that } \mathbf{K}_i \succeq 0, \\ i = 1, \ldots, K, \text{ and } \sum_{i=1}^K \mathbf{K}_i \preceq \mathbf{S} \end{array} \right\}\end{aligned} \tag{315}$$

The secrecy capacity region of the general Gaussian MIMO broadcast channel is given by the following theorem.

**Theorem 7** *The secrecy capacity region of the general Gaussian MIMO multi-receiver wire-tap channel is given by the convex closure of the following union*

$$\bigcup_{\pi \in \Pi} \mathcal{R}^{\text{DPC}}\left(\pi, \mathbf{S}, \{\mathbf{\Sigma}_i\}_{i=1}^K, \mathbf{\Sigma}_Z, \{\mathbf{H}_i\}_{i=1}^K, \mathbf{H}_Z\right) \tag{316}$$

*where* $\Pi$ *is the set of all possible one-to-one permutations on* $\{1, \ldots, K\}$*.*

## 7.1 Proof of Theorem 7

Achievability of the region given in Theorem 7 can be shown by following the achievability proof of Theorem 6 given in Section 6.1, hence it is omitted. For the converse, we basically use the ideas presented in [29, 30]. Following Section V-B of [29], we can construct an equivalent channel which has the same secrecy capacity region as the original channel defined in (13)-(14). In this constructed equivalent channel, all receivers, including the eavesdropper, and the transmitter have the same number of antennas, which is $t$,

$$\hat{\mathbf{Y}}_k = \hat{\mathbf{H}}_k \mathbf{X} + \hat{\mathbf{N}}_k, \quad k = 1, \ldots, K \tag{317}$$

$$\hat{\mathbf{Z}} = \hat{\mathbf{H}}_Z \mathbf{X} + \hat{\mathbf{N}}_Z \tag{318}$$

where $\hat{\mathbf{H}}_k = \hat{\mathbf{\Lambda}}_k \mathbf{V}_k$, $\mathbf{V}_k$ is a $t \times t$ orthonormal matrix, and $\hat{\mathbf{\Lambda}}_k$ is a $t \times t$ diagonal matrix whose first $(t - \hat{r}_k)$ diagonal entries are zero, and the rest of the diagonal entries are strictly positive. Here, $\hat{r}_k$ is the rank of the original channel gain matrix, $\mathbf{H}_k$. The noise covariance matrix of the Gaussian random vector $\hat{\mathbf{N}}_k$ is given by $\hat{\mathbf{\Sigma}}_k$ which has the following block diagonal form

$$\hat{\mathbf{\Sigma}}_k = \begin{bmatrix} \hat{\mathbf{\Sigma}}_k^A & \mathbf{0} \\ \mathbf{0} & \hat{\mathbf{\Sigma}}_k^B \end{bmatrix} \tag{319}$$

where $\hat{\mathbf{\Sigma}}_k^A$ is of size $(t - \hat{r}_k) \times (t - \hat{r}_k)$, and $\hat{\mathbf{\Sigma}}_k^B$ is of size $\hat{r}_k \times \hat{r}_k$.

Similar notations hold for the eavesdropper's observation $\hat{\mathbf{Z}}$ as well. In particular, $\hat{\mathbf{H}}_Z = \hat{\mathbf{\Lambda}}_Z \mathbf{V}_Z$ where $\mathbf{V}_Z$ is a $t \times t$ orthonormal matrix, and $\hat{\mathbf{\Lambda}}_Z$ is a $t \times t$ diagonal matrix whose first $(t - \hat{r}_Z)$ diagonal entries are zero, and the rest of the diagonal entries are strictly positive. Here, $\hat{r}_Z$ is the rank of the original channel gain matrix of the eavesdropper, $\mathbf{H}_Z$. The covariance matrix of the Gaussian random vector $\hat{\mathbf{N}}_Z$ is given by $\hat{\mathbf{\Sigma}}_Z$ which has the following block diagonal form

$$\hat{\mathbf{\Sigma}}_Z = \begin{bmatrix} \hat{\mathbf{\Sigma}}_Z^A & \mathbf{0} \\ \mathbf{0} & \hat{\mathbf{\Sigma}}_Z^B \end{bmatrix} \tag{320}$$

where $\hat{\mathbf{\Sigma}}_Z^A$ is of size $(t - \hat{r}_Z) \times (t - \hat{r}_Z)$ and $\hat{\mathbf{\Sigma}}_Z^B$ is of size $\hat{r}_Z \times \hat{r}_Z$. Since this new channel in (317)-(318) can be constructed from the original channel in (13)-(14) through invertible transformations [29], both have the same secrecy capacity region. Moreover, these transfor-

mations preserve the dirty-paper coding region as well, i.e.,

$$\begin{aligned}
& R_k^{\text{DPC}}\left(\pi, \{\mathbf{K}_i\}_{i=1}^K, \{\mathbf{\Sigma}_i\}_{i=1}^K, \mathbf{\Sigma}_Z, \{\mathbf{H}_i\}_{i=1}^K, \mathbf{H}_Z\right) \\
&= \frac{1}{2}\log\frac{\left|\mathbf{H}_{\pi(k)}\left(\sum_{i=1}^k \mathbf{K}_{\pi(i)}\right)\mathbf{H}_{\pi(k)}^\top + \mathbf{\Sigma}_{\pi(k)}\right|}{\left|\mathbf{H}_{\pi(k)}\left(\sum_{i=1}^{k-1} \mathbf{K}_{\pi(i)}\right)\mathbf{H}_{\pi(k)}^\top + \mathbf{\Sigma}_{\pi(k)}\right|} - \frac{1}{2}\log\frac{\left|\mathbf{H}_Z\left(\sum_{i=1}^k \mathbf{K}_{\pi(i)}\right)\mathbf{H}_Z^\top + \mathbf{\Sigma}_Z\right|}{\left|\mathbf{H}_Z\left(\sum_{i=1}^{k-1} \mathbf{K}_{\pi(i)}\right)\mathbf{H}_Z^\top + \mathbf{\Sigma}_Z\right|} \\
&= \frac{1}{2}\log\frac{\left|\hat{\mathbf{H}}_{\pi(k)}\left(\sum_{i=1}^k \mathbf{K}_{\pi(i)}\right)\hat{\mathbf{H}}_{\pi(k)}^\top + \hat{\mathbf{\Sigma}}_{\pi(k)}\right|}{\left|\hat{\mathbf{H}}_{\pi(k)}\left(\sum_{i=1}^{k-1} \mathbf{K}_{\pi(i)}\right)\hat{\mathbf{H}}_{\pi(k)}^\top + \hat{\mathbf{\Sigma}}_{\pi(k)}\right|} - \frac{1}{2}\log\frac{\left|\hat{\mathbf{H}}_Z\left(\sum_{i=1}^k \mathbf{K}_{\pi(i)}\right)\hat{\mathbf{H}}_Z^\top + \hat{\mathbf{\Sigma}}_Z\right|}{\left|\hat{\mathbf{H}}_Z\left(\sum_{i=1}^{k-1} \mathbf{K}_{\pi(i)}\right)\hat{\mathbf{H}}_Z^\top + \hat{\mathbf{\Sigma}}_Z\right|}, \\
&\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad k = 1, \ldots, K \qquad (321)
\end{aligned}$$

We now define another channel which does not have the same secrecy capacity region or the dirty paper coding region as the original channel:

$$\bar{\mathbf{Y}}_k = \bar{\mathbf{H}}_k\mathbf{X} + \hat{\mathbf{N}}_k, \quad k = 1, \ldots, K \tag{322}$$

$$\bar{\mathbf{Z}} = \bar{\mathbf{H}}_Z\mathbf{X} + \hat{\mathbf{N}}_Z \tag{323}$$

where $\bar{\mathbf{H}}_k = \left(\hat{\mathbf{\Lambda}}_k + \alpha\hat{\mathbf{I}}_k\right)\mathbf{V}_k$ and $\alpha > 0$, and $\hat{\mathbf{I}}_k$ is a $t \times t$ diagonal matrix whose first $(t - \hat{r}_k)$ diagonal entries are 1, and the rest of the diagonal entries are zero. Similarly, $\bar{\mathbf{H}}_Z = \left(\hat{\mathbf{\Lambda}}_Z + \alpha\hat{\mathbf{I}}_Z\right)\mathbf{V}_Z$, where $\hat{\mathbf{I}}_Z$ is a $t \times t$ diagonal matrix whose first $(t - \hat{r}_Z)$ diagonal entries are 1, and the rest are zero. We note that $\{\bar{\mathbf{H}}_k\}_{k=1}^K, \bar{\mathbf{H}}_Z$ are invertible, hence the channel defined by (322)-(323) can be considered as an aligned Gaussian MIMO multi-receiver wiretap channel. Thus, since it is an aligned Gaussian MIMO multi-receiver wiretap channel, its secrecy capacity region is given by Theorem 6.

We now show that as $\alpha \to 0$, the secrecy capacity region of the channel described by (322)-(323) converges to a region that includes the secrecy capacity region of the original channel in (13)-(14). Since the original channel in (13)-(14) and the channel in (317)-(318) have the same secrecy capacity region and the dirty-paper coding region, checking that the secrecy capacity region of the channel described by (322)-(323) converges, as $\alpha \to 0$, to a region that includes the secrecy capacity region of the channel described by (317)-(318), is sufficient. To this end, consider an arbitrary $(2^{nR_1}, \ldots, 2^{nR_K}, n)$ code which can be transmitted with vanishingly small probability of error and in perfect secrecy when it is used in the channel given in (317)-(318). We will show that the same code can also be transmitted with vanishingly small probability of error and in perfect secrecy when it is used in the channel given in (322)-(323) as $\alpha \to 0$. This will imply that the secrecy capacity region of the channel given in (322)-(323) converges to a region that includes the secrecy

capacity region of the channel given in (317)-(318). We first note that

$$\bar{\mathbf{Y}}_k = \left(\hat{\mathbf{\Lambda}}_k + \alpha\hat{\mathbf{I}}_k\right)\mathbf{V}_k\mathbf{X} + \hat{\mathbf{N}}_k \tag{324}$$

$$= \begin{bmatrix} \alpha\hat{\mathbf{I}}_k^A\mathbf{V}_k\mathbf{X} \\ \hat{\mathbf{\Lambda}}_k^B\mathbf{V}_k\mathbf{X} \end{bmatrix} + \begin{bmatrix} \hat{\mathbf{N}}_k^A \\ \hat{\mathbf{N}}_k^B \end{bmatrix} \tag{325}$$

$$= \begin{bmatrix} \bar{\mathbf{Y}}_k^A \\ \bar{\mathbf{Y}}_k^B \end{bmatrix}, \qquad k = 1, \ldots, K \tag{326}$$

where $\hat{\mathbf{I}}_k^A$ contains the first $(t - \hat{r}_k)$ rows of $\hat{\mathbf{I}}_k$, and $\hat{\mathbf{\Lambda}}_k^B$ contains the last $\hat{r}_k$ rows of $\hat{\mathbf{\Lambda}}_k$. $\hat{\mathbf{N}}_k^A$ is a Gaussian random vector that contains the first $(t - \hat{r}_k)$ entries of $\hat{\mathbf{N}}_k$, and $\hat{\mathbf{N}}_k^B$ is a vector that contains the last $\hat{r}_k$ entries. The covariance matrices of $\hat{\mathbf{N}}_k^A, \hat{\mathbf{N}}_k^B$ are $\hat{\mathbf{\Sigma}}_k^A, \hat{\mathbf{\Sigma}}_k^B$, respectively, and $\hat{\mathbf{N}}_k^A$ and $\hat{\mathbf{N}}_k^B$ are independent as can be observed through (319). Similarly, we can write

$$\hat{\mathbf{Y}}_k = \hat{\mathbf{\Lambda}}_k\mathbf{V}_k\mathbf{X} + \hat{\mathbf{N}}_k \tag{327}$$

$$= \begin{bmatrix} \mathbf{0} \\ \hat{\mathbf{\Lambda}}_k^B\mathbf{V}_k\mathbf{X} \end{bmatrix} + \begin{bmatrix} \hat{\mathbf{N}}_k^A \\ \hat{\mathbf{N}}_k^B \end{bmatrix} \tag{328}$$

$$= \begin{bmatrix} \hat{\mathbf{Y}}_k^A \\ \hat{\mathbf{Y}}_k^B \end{bmatrix}, \qquad k = 1, \ldots, K \tag{329}$$

We note that $\bar{\mathbf{Y}}_k^B = \hat{\mathbf{Y}}_k^B,\ k = 1, \ldots, K$, thus we have

$$\mathbf{X} \to \bar{\mathbf{Y}}_k \to \hat{\mathbf{Y}}_k, \quad k = 1, \ldots, K \tag{330}$$

which ensures the any message rate that is decodable by the $k$th user of the channel given in (317)-(318) is also decodable by the $k$th user of the channel given in (322)-(323). Thus, any $(2^{nR_1}, \ldots, 2^{nR_K}, n)$ code which can be transmitted with vanishingly small probability of error in the channel defined by (317)-(318) can be transmitted with vanishingly small probability of error in the channel defined by (322)-(323) as well.

We now check the secrecy constraints. To this end, we note that

$$\bar{\mathbf{Z}} = \left(\hat{\mathbf{\Lambda}}_Z + \alpha\hat{\mathbf{I}}_Z\right)\mathbf{V}_Z\mathbf{X} + \hat{\mathbf{N}}_Z \tag{331}$$

$$= \begin{bmatrix} \alpha\hat{\mathbf{I}}_Z^A\mathbf{V}_Z\mathbf{X} \\ \hat{\mathbf{\Lambda}}_Z^B\mathbf{V}_Z\mathbf{X} \end{bmatrix} + \begin{bmatrix} \hat{\mathbf{N}}_Z^A \\ \hat{\mathbf{N}}_Z^B \end{bmatrix} \tag{332}$$

$$= \begin{bmatrix} \bar{\mathbf{Z}}^A \\ \bar{\mathbf{Z}}^B \end{bmatrix} \tag{333}$$

where $\hat{\mathbf{I}}_Z^A$ contains the first $(t - \hat{r}_Z)$ rows of $\hat{\mathbf{I}}_Z$, and $\hat{\mathbf{\Lambda}}_Z^B$ contains the last $\hat{r}_Z$ rows of $\hat{\mathbf{\Lambda}}_Z$. $\hat{\mathbf{N}}_Z^A$ is a Gaussian random vector that contains the first $t - \hat{r}_Z$ entries of $\hat{\mathbf{N}}_Z$, and $\hat{\mathbf{N}}_Z^B$ is a

vector that contains the last $\hat{r}_Z$ entries. The covariance matrices of $\hat{\mathbf{N}}_Z^A, \hat{\mathbf{N}}_Z^B$ are $\hat{\mathbf{\Sigma}}_Z^A, \hat{\mathbf{\Sigma}}_Z^B$, respectively, and $\hat{\mathbf{N}}_Z^A$ and $\hat{\mathbf{N}}_Z^B$ are independent as can be observed through (320). Similarly, we can write

$$\hat{\mathbf{Z}} = \hat{\mathbf{\Lambda}}_Z \mathbf{V}_Z \mathbf{X} + \hat{\mathbf{N}}_Z \tag{334}$$

$$= \begin{bmatrix} \mathbf{0} \\ \hat{\mathbf{\Lambda}}_Z^B \mathbf{V}_Z \mathbf{X} \end{bmatrix} + \begin{bmatrix} \hat{\mathbf{N}}_Z^A \\ \hat{\mathbf{N}}_Z^B \end{bmatrix} \tag{335}$$

$$= \begin{bmatrix} \hat{\mathbf{Z}}^A \\ \hat{\mathbf{Z}}^B \end{bmatrix} \tag{336}$$

We note that $\bar{\mathbf{Z}}^B = \hat{\mathbf{Z}}^B$, and thus we have

$$\mathbf{X} \rightarrow \bar{\mathbf{Z}} \rightarrow \hat{\mathbf{Z}} \tag{337}$$

We now show that any $(2^{nR_1}, \ldots, 2^{nR_K})$ code that achieves the perfect secrecy rates $(R_1, \ldots, R_K)$ in the channel given in (317)-(318) also achieves the same perfect secrecy rates in the channel given in (322)-(323) when $\alpha \rightarrow 0$. To this end, let $\mathcal{S}$ be a non-empty subset of $\{1, \ldots, K\}$. We consider the following equivocation

$$H(W_{\mathcal{S}}|\bar{\mathbf{Z}}^n) = H(W_{\mathcal{S}}) - I(W_{\mathcal{S}}; \bar{\mathbf{Z}}^n) \tag{338}$$

$$= H(W_{\mathcal{S}}|\hat{\mathbf{Z}}^n) + I(W_{\mathcal{S}}; \hat{\mathbf{Z}}^n) - I(W_{\mathcal{S}}; \bar{\mathbf{Z}}^n) \tag{339}$$

$$= H(W_{\mathcal{S}}|\hat{\mathbf{Z}}^{A,n}, \hat{\mathbf{Z}}^{B,n}) + I(W_{\mathcal{S}}; \hat{\mathbf{Z}}^{A,n}, \hat{\mathbf{Z}}^{B,n}) - I(W_{\mathcal{S}}; \bar{\mathbf{Z}}^{A,n}, \bar{\mathbf{Z}}^{B,n}) \tag{340}$$

$$= H(W_{\mathcal{S}}|\hat{\mathbf{Z}}^{A,n}, \hat{\mathbf{Z}}^{B,n}) + I(W_{\mathcal{S}}; \hat{\mathbf{Z}}^{B,n}) - I(W_{\mathcal{S}}; \bar{\mathbf{Z}}^{A,n}, \hat{\mathbf{Z}}^{B,n}) \tag{341}$$

$$= H(W_{\mathcal{S}}|\hat{\mathbf{Z}}^{A,n}, \hat{\mathbf{Z}}^{B,n}) - I(W_{\mathcal{S}}; \bar{\mathbf{Z}}^{A,n}|\hat{\mathbf{Z}}^{B,n}) \tag{342}$$

where (341) follows from the facts that $W_{\mathcal{S}}$ and $\hat{\mathbf{Z}}^{A,n} = \hat{\mathbf{N}}^{A,n}$ are independent, and $\bar{\mathbf{Z}}^{B,n} =$

$\hat{\mathbf{Z}}^{B,n}$. We now bound the mutual information term in (342)

$$
\begin{aligned}
I(W_{\mathcal{S}};\bar{\mathbf{Z}}^{A,n}|\hat{\mathbf{Z}}^{B,n}) &\leq I(\mathbf{X}^n;\bar{\mathbf{Z}}^{A,n}|\hat{\mathbf{Z}}^{B,n}) && (343)\\
&= h(\bar{\mathbf{Z}}^{A,n}|\hat{\mathbf{Z}}^{B,n}) - h(\bar{\mathbf{Z}}^{A,n}|\hat{\mathbf{Z}}^{B,n},\mathbf{X}^n) && (344)\\
&= h(\bar{\mathbf{Z}}^{A,n}|\hat{\mathbf{Z}}^{B,n}) - h(\bar{\mathbf{Z}}^{A,n}|\mathbf{X}^n) && (345)\\
&\leq h(\bar{\mathbf{Z}}^{A,n}) - h(\bar{\mathbf{Z}}^{A,n}|\mathbf{X}^n) && (346)\\
&= I(\mathbf{X}^n;\bar{\mathbf{Z}}^{A,n}) && (347)\\
&\leq \sum_{i=1}^{n} I(\mathbf{X}_i;\bar{\mathbf{Z}}_i^A) && (348)\\
&\leq \sum_{i=1}^{n} \max_{E[\mathbf{X}_i\mathbf{X}_i^\top]\preceq\mathbf{S}} I(\mathbf{X}_i;\bar{\mathbf{Z}}_i^A) && (349)\\
&\leq \sum_{i=1}^{n} \frac{1}{2}\log\frac{\left|\alpha^2\hat{\mathbf{I}}_Z^A\mathbf{V}_Z\mathbf{S}\mathbf{V}_Z^\top(\hat{\mathbf{I}}_Z^A)^\top+\hat{\boldsymbol{\Sigma}}_Z^A\right|}{\left|\hat{\boldsymbol{\Sigma}}_Z^A\right|} && (350)\\
&= \frac{n}{2}\log\frac{\left|\alpha^2\hat{\mathbf{I}}_Z^A\mathbf{V}_Z\mathbf{S}\mathbf{V}_Z^\top(\hat{\mathbf{I}}_Z^A)^\top+\hat{\boldsymbol{\Sigma}}_Z^A\right|}{\left|\hat{\boldsymbol{\Sigma}}_Z^A\right|} && (351)
\end{aligned}
$$

where (343) follows from the Markov chain $W_{\mathcal{S}} \rightarrow \mathbf{X}^n \rightarrow (\bar{\mathbf{Z}}^{A,n},\hat{\mathbf{Z}}^{B,n})$, (345) is due to the Markov chain $\bar{\mathbf{Z}}^{A,n} \rightarrow \mathbf{X}^n \rightarrow \hat{\mathbf{Z}}^{B,n}$, (346) comes from the fact that conditioning cannot increase entropy, (348) is a consequence of the fact that channel is memoryless, (350) is due to the fact that subject to a covariance constraint, Gaussian distribution maximizes the differential entropy. Thus, plugging (351) into (342) yields

$$
\frac{1}{n}H(W_{\mathcal{S}}|\bar{\mathbf{Z}}^n) \geq \frac{1}{n}H(W_{\mathcal{S}}|\hat{\mathbf{Z}}^n) - \frac{1}{2}\log\frac{\left|\alpha^2\hat{\mathbf{I}}_Z^A\mathbf{V}_Z\mathbf{S}\mathbf{V}_Z^\top(\hat{\mathbf{I}}_Z^A)^\top+\hat{\boldsymbol{\Sigma}}_Z^A\right|}{\left|\hat{\boldsymbol{\Sigma}}_Z^A\right|} \tag{352}
$$

which implies that

$$
\begin{aligned}
\lim_{n\rightarrow\infty}\frac{1}{n}H(W_{\mathcal{S}}|\bar{\mathbf{Z}}^n) &\geq \lim_{n\rightarrow\infty}\frac{1}{n}H(W_{\mathcal{S}}|\hat{\mathbf{Z}}^n) - \lim_{\alpha\rightarrow 0}\frac{1}{2}\log\frac{\left|\alpha^2\hat{\mathbf{I}}_Z^A\mathbf{V}_Z\mathbf{S}\mathbf{V}_Z^\top(\hat{\mathbf{I}}_Z^A)^\top+\hat{\boldsymbol{\Sigma}}_Z^A\right|}{\left|\hat{\boldsymbol{\Sigma}}_Z^A\right|} && (353)\\
&= \lim_{n\rightarrow\infty}\frac{1}{n}H(W_{\mathcal{S}}|\hat{\mathbf{Z}}^n) && (354)\\
&\geq \sum_{k\in\mathcal{S}} R_k && (355)
\end{aligned}
$$

where (354) follows from the fact that $\log|\alpha^2\mathbf{A}+\mathbf{B}|$ is continuous in $\alpha$ for positive definite matrices $\mathbf{A},\mathbf{B}$, and (355) comes from our assumption that the codebook under consideration achieves perfect secrecy in the channel given in (317)-(318). Thus, we have shown that

if a codebook achieves the perfect secrecy rates $(R_1, \ldots, R_K)$ in the channel defined by (317)-(318), then it also achieves the same perfect secrecy rates in the channel defined by (322)-(323) as $\alpha \to 0$. Thus, the secrecy capacity region of the latter channel converges to a region that includes the secrecy capacity region of the channel in (317)-(318), and also the secrecy capacity region of the original channel in (13)-(14). Since the channel in (322)-(323) is an aligned channel, its secrecy capacity region is given by Theorem 6, and it is equal to the dirty-paper coding region. Thus, to find the region that the secrecy capacity region of the channel in (322)-(323) converges to as $\alpha \to 0$, it is sufficient to consider the region which the dirty-paper coding region converges to as $\alpha \to 0$. For that purpose, pick the $k$th user, and the identity encoding order, i.e., $\pi(k) = k, \; k = 1, \ldots, K$. The corresponding secrecy rate is

$$\begin{aligned}
&\frac{1}{2}\log\frac{\left|\bar{\mathbf{H}}_{\pi(k)}\left(\sum_{i=1}^{k}\mathbf{K}_{\pi(i)}\right)\bar{\mathbf{H}}_{\pi(k)}^{\top}+\hat{\boldsymbol{\Sigma}}_{\pi(k)}\right|}{\left|\bar{\mathbf{H}}_{\pi(k)}\left(\sum_{i=1}^{k-1}\mathbf{K}_{\pi(i)}\right)\bar{\mathbf{H}}_{\pi(k)}^{\top}+\hat{\boldsymbol{\Sigma}}_{\pi(k)}\right|}-\frac{1}{2}\log\frac{\left|\bar{\mathbf{H}}_{Z}\left(\sum_{i=1}^{k}\mathbf{K}_{\pi(i)}\right)\bar{\mathbf{H}}_{Z}^{\top}+\hat{\boldsymbol{\Sigma}}_{Z}\right|}{\left|\bar{\mathbf{H}}_{Z}\left(\sum_{i=1}^{k-1}\mathbf{K}_{\pi(i)}\right)\bar{\mathbf{H}}_{Z}^{\top}+\hat{\boldsymbol{\Sigma}}_{Z}\right|}\\
&=\frac{1}{2}\log\frac{\left|\left(\hat{\mathbf{H}}_{\pi(k)}+\alpha\hat{\mathbf{I}}_{\pi(k)}\mathbf{V}_{\pi(k)}\right)\left(\sum_{i=1}^{k}\mathbf{K}_{\pi(i)}\right)\left(\hat{\mathbf{H}}_{\pi(k)}+\alpha\hat{\mathbf{I}}_{\pi(k)}\mathbf{V}_{\pi(k)}\right)^{\top}+\hat{\boldsymbol{\Sigma}}_{\pi(k)}\right|}{\left|\left(\hat{\mathbf{H}}_{\pi(k)}+\alpha\hat{\mathbf{I}}_{\pi(k)}\mathbf{V}_{\pi(k)}\right)\left(\sum_{i=1}^{k-1}\mathbf{K}_{\pi(i)}\right)\left(\hat{\mathbf{H}}_{\pi(k)}+\alpha\hat{\mathbf{I}}_{\pi(k)}\mathbf{V}_{\pi(k)}\right)^{\top}+\hat{\boldsymbol{\Sigma}}_{\pi(k)}\right|}\\
&\quad-\frac{1}{2}\log\frac{\left|\left(\hat{\mathbf{H}}_{Z}+\alpha\hat{\mathbf{I}}_{Z}\mathbf{V}_{Z}\right)\left(\sum_{i=1}^{k}\mathbf{K}_{\pi(i)}\right)\left(\hat{\mathbf{H}}_{Z}+\alpha\hat{\mathbf{I}}_{Z}\mathbf{V}_{Z}\right)^{\top}+\hat{\boldsymbol{\Sigma}}_{Z}\right|}{\left|\left(\hat{\mathbf{H}}_{Z}+\alpha\hat{\mathbf{I}}_{Z}\mathbf{V}_{Z}\right)\left(\sum_{i=1}^{k-1}\mathbf{K}_{\pi(i)}\right)\left(\hat{\mathbf{H}}_{Z}+\alpha\hat{\mathbf{I}}_{Z}\mathbf{V}_{Z}\right)^{\top}+\hat{\boldsymbol{\Sigma}}_{Z}\right|}
\end{aligned}\tag{356}$$

which converges to

$$\frac{1}{2}\log\frac{\left|\hat{\mathbf{H}}_{\pi(k)}\left(\sum_{i=1}^{k}\mathbf{K}_{\pi(i)}\right)\hat{\mathbf{H}}_{\pi(k)}^{\top}+\hat{\boldsymbol{\Sigma}}_{\pi(k)}\right|}{\left|\hat{\mathbf{H}}_{\pi(k)}\left(\sum_{i=1}^{k-1}\mathbf{K}_{\pi(i)}\right)\hat{\mathbf{H}}_{\pi(k)}^{\top}+\hat{\boldsymbol{\Sigma}}_{\pi(k)}\right|}-\frac{1}{2}\log\frac{\left|\hat{\mathbf{H}}_{Z}\left(\sum_{i=1}^{k}\mathbf{K}_{\pi(i)}\right)\hat{\mathbf{H}}_{Z}^{\top}+\hat{\boldsymbol{\Sigma}}_{Z}\right|}{\left|\hat{\mathbf{H}}_{Z}\left(\sum_{i=1}^{k-1}\mathbf{K}_{\pi(i)}\right)\hat{\mathbf{H}}_{Z}^{\top}+\hat{\boldsymbol{\Sigma}}_{Z}\right|}\tag{357}$$

as $\alpha \to 0$ due to the continuity of $\log|\cdot|$ in positive semi-definite matrices. Moreover, (357) is equal to

$$\frac{1}{2}\log\frac{\left|\mathbf{H}_{\pi(k)}\left(\sum_{i=1}^{k}\mathbf{K}_{\pi(i)}\right)\mathbf{H}_{\pi(k)}^{\top}+\boldsymbol{\Sigma}_{\pi(k)}\right|}{\left|\mathbf{H}_{\pi(k)}\left(\sum_{i=1}^{k-1}\mathbf{K}_{\pi(i)}\right)\mathbf{H}_{\pi(k)}^{\top}+\boldsymbol{\Sigma}_{\pi(k)}\right|}-\frac{1}{2}\log\frac{\left|\mathbf{H}_{Z}\left(\sum_{i=1}^{k}\mathbf{K}_{\pi(i)}\right)\mathbf{H}_{Z}^{\top}+\boldsymbol{\Sigma}_{Z}\right|}{\left|\mathbf{H}_{Z}\left(\sum_{i=1}^{k-1}\mathbf{K}_{\pi(i)}\right)\mathbf{H}_{Z}^{\top}+\boldsymbol{\Sigma}_{Z}\right|}\tag{358}$$

which implies that the secrecy capacity region of the general Gaussian MIMO multi-receiver wiretap channel is given by the dirty-paper coding region, completing the proof.

# 8 Conclusions

We characterized the secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel. We showed that it is achievable with a variant of dirty-paper coding with Gaussian signals. Before reaching this result, we first visited the scalar case, and showed the necessity of a new proof technique for the converse. In particular, we showed that the extensions of existing converses for the Gaussian scalar broadcast channels fall short of resolving the ambiguity regarding the auxiliary random variables. We showed that, unlike the stand-alone use of the entropy-power inequality [24, 25], the use of the relationships either between the MMSE and the mutual information or between the Fisher information and the differential entropy resolves this ambiguity. Extending this methodology to degraded vector channels, we found the secrecy capacity region of the degraded Gaussian MIMO multi-receiver wiretap channel. Once we obtained the secrecy capacity region of the degraded MIMO channel, we generalized it to arbitrary channels by using the channel enhancement method and some limiting arguments as in [29, 30].

# Appendices

## A Proof of Lemma 11

Let $\rho_i(\mathbf{x}|\mathbf{u}) = \frac{\partial \log f(\mathbf{x}|\mathbf{u})}{\partial x_i}$, i.e., the $i$th component of $\boldsymbol{\rho}(\mathbf{x}|\mathbf{u})$. Then, we have

$$E\left[g(\mathbf{X})\rho_i(\mathbf{X}|\mathbf{U})\right] = \int g(\mathbf{x}) \frac{\frac{\partial f(\mathbf{x}|\mathbf{u})}{\partial x_i}}{f(\mathbf{x}|\mathbf{u})} f(\mathbf{x}, \mathbf{u})\, d\mathbf{x}\, d\mathbf{u} \tag{359}$$

$$= \int g(\mathbf{x}) \frac{\partial f(\mathbf{x}|\mathbf{u})}{\partial x_i} f(\mathbf{u})\, d\mathbf{x}\, d\mathbf{u} \tag{360}$$

$$= \int \left[ \int_{-\infty}^{+\infty} g(\mathbf{x}) \frac{\partial f(\mathbf{x}|\mathbf{u})}{\partial x_i} dx_i \right] f(\mathbf{u})\, d\mathbf{x}^-\, d\mathbf{u} \tag{361}$$

where $d\mathbf{x}^- = dx_1 \ldots dx_{i-1} dx_{i+1} \ldots dx_n$. The inner integral can be evaluated using integration by parts as

$$\int_{-\infty}^{+\infty} g(\mathbf{x}) \frac{\partial f(\mathbf{x}|\mathbf{u})}{\partial x_i} dx_i = \left[ g(\mathbf{x}) f(\mathbf{x}|\mathbf{u}) \right] \Big|_{x_i=-\infty}^{+\infty} - \int_{-\infty}^{+\infty} f(\mathbf{x}|\mathbf{u}) \frac{\partial g(\mathbf{x})}{\partial x_i} dx_i \tag{362}$$

$$= - \int_{-\infty}^{+\infty} f(\mathbf{x}|\mathbf{u}) \frac{\partial g(\mathbf{x})}{\partial x_i} dx_i \tag{363}$$

where (363) comes from the assumption in (183). Plugging (363) into (361) yields

$$E\left[g(\mathbf{X})\rho_i(\mathbf{X}|\mathbf{U})\right] = -\int \frac{\partial g(\mathbf{x})}{\partial x_i} f(\mathbf{x},\mathbf{u})\ d\mathbf{x}\ d\mathbf{u} \tag{364}$$

$$= -E\left[\frac{\partial g(\mathbf{x})}{\partial x_i}\right] \tag{365}$$

which concludes the proof.

# B Proof of Lemma 12

Let $\rho_i(\mathbf{x}|\mathbf{u}) = \frac{\partial \log f(\mathbf{x}|\mathbf{u})}{\partial x_i}$, i.e., the $i$th component of $\boldsymbol{\rho}(\mathbf{x}|\mathbf{u})$. Then, we have

$$E\left[\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})|\mathbf{U}=\mathbf{u}\right] = \int \frac{\frac{\partial f(\mathbf{x}|\mathbf{u})}{\partial x_i}}{f(\mathbf{x}|\mathbf{u})} f(\mathbf{x}|\mathbf{u}) d\mathbf{x} \tag{366}$$

$$= \int \left[\int_{-\infty}^{+\infty} \frac{\partial f(\mathbf{x}|\mathbf{u})}{\partial x_i} dx_i\right] d\mathbf{x}^- \tag{367}$$

where $d\mathbf{x}^- = dx_1 \dots dx_{i-1} dx_{i+1} \dots dx_n$. The inner integral is

$$\int_{-\infty}^{+\infty} \frac{\partial f(\mathbf{x}|\mathbf{u})}{\partial x_i} dx_i = f(\mathbf{x}|\mathbf{u})\Big|_{x_i=-\infty}^{+\infty} = 0 \tag{368}$$

since $f(\mathbf{x}|\mathbf{u})$ is a valid probability density function. This completes the proof of the first part. For the second part, we have

$$E\left[g(\mathbf{U})\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})\right] = E\left[g(\mathbf{U})E\big[\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})|\mathbf{U}=\mathbf{u}\big]\right] = 0 \tag{369}$$

where the second equality follows from the fact that the inner expectation is zero as the first part of this lemma states. The last part of the lemma follows by selecting $g(\mathbf{U}) = E\left[\mathbf{X}|\mathbf{U}\right]$ in the second part of this lemma.

# C Proof of Lemma 14

Throughout this proof, the subscript of $f$ will denote the random vector for which $f$ is the density. For example, $f_X(\mathbf{x}|\mathbf{u})$ is the conditional density of $\mathbf{X}$. We first note that

$$f_W(\mathbf{w}|\mathbf{u}) = \int f_{X,W}(\mathbf{x},\mathbf{w}|\mathbf{u}) d\mathbf{x} = \int f_X(\mathbf{x}|\mathbf{u}) f_Y(\mathbf{w}-\mathbf{x}|\mathbf{u}) d\mathbf{x} \tag{370}$$

where the second equality is due to the conditional independence of $\mathbf{X}$ and $\mathbf{Y}$ given $\mathbf{U}$. Differentiating both sides of (370), we get

$$\frac{\partial f_W(\mathbf{w}|\mathbf{u})}{\partial w_i} = \int f_X(\mathbf{x}|\mathbf{u})\frac{\partial f_Y(\mathbf{w}-\mathbf{x}|\mathbf{u})}{\partial w_i}d\mathbf{x} \tag{371}$$

$$= -\int f_X(\mathbf{x}|\mathbf{u})\frac{\partial f_Y(\mathbf{w}-\mathbf{x}|\mathbf{u})}{\partial x_i}d\mathbf{x} \tag{372}$$

$$= \Big[-f_X(\mathbf{x}|\mathbf{u})f_Y(\mathbf{w}-\mathbf{x}|\mathbf{u})\Big]\Big|_{x_i=-\infty}^{\infty} + \int f_Y(\mathbf{w}-\mathbf{x}|\mathbf{u})\frac{\partial f_X(\mathbf{x}|\mathbf{u})}{\partial x_i}d\mathbf{x} \tag{373}$$

$$= \int f_Y(\mathbf{w}-\mathbf{x}|\mathbf{u})\frac{\partial f_X(\mathbf{x}|\mathbf{u})}{\partial x_i}d\mathbf{x} \tag{374}$$

where (372) is due to

$$\frac{\partial f_Y(\mathbf{w}-\mathbf{x}|\mathbf{u})}{\partial w_i} = \frac{\partial f_Y(\mathbf{w}-\mathbf{x}|\mathbf{u})}{\partial(w_i-x_i)}\frac{\partial(w_i-x_i)}{\partial w_i} \tag{375}$$

$$= -\frac{\partial f_Y(\mathbf{w}-\mathbf{x}|\mathbf{u})}{\partial(w_i-x_i)}\frac{\partial(w_i-x_i)}{\partial x_i} \tag{376}$$

$$= -\frac{\partial f_Y(\mathbf{w}-\mathbf{x}|\mathbf{u})}{\partial x_i} \tag{377}$$

and (373) follows from the fact that $f_X(\mathbf{x}|\mathbf{u}), f_Y(\mathbf{w}-\mathbf{x}|\mathbf{u})$ vanish at infinity since they are probability density functions. Using (374), we get

$$\boldsymbol{\rho}_i(\mathbf{w}|\mathbf{u}) = \frac{\frac{\partial f_W(\mathbf{w}|\mathbf{u})}{\partial w_i}}{f_W(\mathbf{w}|\mathbf{u})} = \int \frac{f_Y(\mathbf{w}-\mathbf{x}|\mathbf{u})}{f_W(\mathbf{w}|\mathbf{u})}\frac{\partial f_X(\mathbf{x}|\mathbf{u})}{\partial x_i}d\mathbf{x} \tag{378}$$

$$= \int \frac{f_X(\mathbf{x}|\mathbf{u})f_Y(\mathbf{w}-\mathbf{x}|\mathbf{u})}{f_W(\mathbf{w}|\mathbf{u})}\frac{\frac{\partial f_X(\mathbf{x}|\mathbf{u})}{\partial x_i}}{f_X(\mathbf{x}|\mathbf{u})}d\mathbf{x} \tag{379}$$

$$= \int f_X(\mathbf{x}|\mathbf{u},\mathbf{w})\frac{\frac{\partial f_X(\mathbf{x}|\mathbf{u})}{\partial x_i}}{f_X(\mathbf{x}|\mathbf{u})}d\mathbf{x} \tag{380}$$

$$= E\left[\frac{1}{f_X(\mathbf{x}|\mathbf{u})}\;\frac{\partial f_X(\mathbf{x}|\mathbf{u})}{\partial x_i}\middle|\mathbf{W}=\mathbf{w},\mathbf{U}=\mathbf{u}\right] \tag{381}$$

where (380) follows from the fact that

$$f_X(\mathbf{x}|\mathbf{u},\mathbf{w}) = \frac{f_{X,W}(\mathbf{x},\mathbf{w}|\mathbf{u})}{f_W(\mathbf{w}|\mathbf{u})} = \frac{f_X(\mathbf{x}|\mathbf{u})f_Y(\mathbf{w}-\mathbf{x}|\mathbf{u})}{f_W(\mathbf{w}|\mathbf{u})} \tag{382}$$

Equation (381) implies

$$\boldsymbol{\rho}(\mathbf{w}|\mathbf{u}) = E\left[\boldsymbol{\rho}(\mathbf{X}|\mathbf{U}=\mathbf{u})|\mathbf{W}=\mathbf{w},\mathbf{U}=\mathbf{u}\right] \tag{383}$$

and due to symmetry, we also have

$$\boldsymbol{\rho}(\mathbf{w}|\mathbf{u}) = E\left[\boldsymbol{\rho}(\mathbf{Y}|\mathbf{U}=\mathbf{u})|\mathbf{W}=\mathbf{w},\mathbf{U}=\mathbf{u}\right] \tag{384}$$

which completes the proof.

# D Proof of Lemma 15

Let $\mathbf{W} = \mathbf{X} + \mathbf{Y}$. We have

$$\begin{aligned}
\mathbf{0} \preceq E\Big[&\Big(\mathbf{A}\boldsymbol{\rho}(\mathbf{X}|\mathbf{U}) + (\mathbf{I}-\mathbf{A})\boldsymbol{\rho}(\mathbf{Y}|\mathbf{U}) - \boldsymbol{\rho}(\mathbf{W}|\mathbf{U})\Big) \\
&\qquad \Big(\mathbf{A}\boldsymbol{\rho}(\mathbf{X}|\mathbf{U}) + (\mathbf{I}-\mathbf{A})\boldsymbol{\rho}(\mathbf{Y}|\mathbf{U}) - \boldsymbol{\rho}(\mathbf{W}|\mathbf{U})\Big)^{\top}\Big] &(385)\\
&= \mathbf{A}E\left[\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})^{\top}\right]\mathbf{A}^{\top} + \mathbf{A}E\left[\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})\boldsymbol{\rho}(\mathbf{Y}|\mathbf{U})^{\top}\right](\mathbf{I}-\mathbf{A})^{\top} \\
&\quad - \mathbf{A}E\left[\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})\boldsymbol{\rho}(\mathbf{W}|\mathbf{U})^{\top}\right] + (\mathbf{I}-\mathbf{A})E\left[\boldsymbol{\rho}(\mathbf{Y}|\mathbf{U})\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})^{\top}\right]\mathbf{A}^{\top} \\
&\quad + (\mathbf{I}-\mathbf{A})E\left[\boldsymbol{\rho}(\mathbf{Y}|\mathbf{U})\boldsymbol{\rho}(\mathbf{Y}|\mathbf{U})^{\top}\right](\mathbf{I}-\mathbf{A})^{\top} - (\mathbf{I}-\mathbf{A})E\left[\boldsymbol{\rho}(\mathbf{Y}|\mathbf{U})\boldsymbol{\rho}(\mathbf{W}|\mathbf{U})^{\top}\right] \\
&\quad - E\left[\boldsymbol{\rho}(\mathbf{W}|\mathbf{U})\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})^{\top}\right]\mathbf{A}^{\top} - E\left[\boldsymbol{\rho}(\mathbf{W}|\mathbf{U})\boldsymbol{\rho}(\mathbf{Y}|\mathbf{U})^{\top}\right](\mathbf{I}-\mathbf{A})^{\top} \\
&\quad + E\left[\boldsymbol{\rho}(\mathbf{W}|\mathbf{U})\boldsymbol{\rho}(\mathbf{W}|\mathbf{U})^{\top}\right] &(386)
\end{aligned}$$

We note that, from the definition of the conditional Fisher information matrix, we have

$$E\left[\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})^{\top}\right] = \mathbf{J}(\mathbf{X}|\mathbf{U}) \tag{387}$$

$$E\left[\boldsymbol{\rho}(\mathbf{Y}|\mathbf{U})\boldsymbol{\rho}(\mathbf{Y}|\mathbf{U})^{\top}\right] = \mathbf{J}(\mathbf{Y}|\mathbf{U}) \tag{388}$$

$$E\left[\boldsymbol{\rho}(\mathbf{W}|\mathbf{U})\boldsymbol{\rho}(\mathbf{W}|\mathbf{U})^{\top}\right] = \mathbf{J}(\mathbf{W}|\mathbf{U}) \tag{389}$$

Moreover, we have

$$\begin{aligned}
E\left[\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})\boldsymbol{\rho}(\mathbf{Y}|\mathbf{U})^{\top}\right] &= \left(E\left[\boldsymbol{\rho}(\mathbf{Y}|\mathbf{U})\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})^{\top}\right]\right)^{\top} &(390)\\
&= \left(E\left[E\left[\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})\big|\mathbf{U}=\mathbf{u}\right]E\left[\boldsymbol{\rho}(\mathbf{Y}|\mathbf{U})\big|\mathbf{U}=\mathbf{u}\right]\right]\right)^{\top} &(391)\\
&= \mathbf{0} &(392)
\end{aligned}$$

where (391) comes from the fact that given $\mathbf{U} = \mathbf{u}$, $\mathbf{X}$ and $\mathbf{Y}$ are conditionally independent, and (392) follows from the first part of Lemma 12, namely

$$E\left[\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})\big|\mathbf{U}=\mathbf{u}\right] = E\left[\boldsymbol{\rho}(\mathbf{Y}|\mathbf{U})\big|\mathbf{U}=\mathbf{u}\right] = \mathbf{0} \tag{393}$$

Furthermore, we have

$$E\left[\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})\boldsymbol{\rho}(\mathbf{W}|\mathbf{U})^\top\right] = E\left[E\left[\boldsymbol{\rho}(\mathbf{X}|\mathbf{U}=\mathbf{u})\middle|\mathbf{W}=\mathbf{w},\mathbf{U}=\mathbf{u}\right]\boldsymbol{\rho}(\mathbf{W}|\mathbf{U})^\top\right] \tag{394}$$

$$= E\left[\boldsymbol{\rho}(\mathbf{W}|\mathbf{U})\boldsymbol{\rho}(\mathbf{W}|\mathbf{U})^\top\right] \tag{395}$$

$$= \mathbf{J}(\mathbf{W}|\mathbf{U}) \tag{396}$$

where (395) follows from Lemma 14, and (396) comes from the definition of the conditional Fisher information matrix. Similarly, we also have

$$E\left[\boldsymbol{\rho}(\mathbf{Y}|\mathbf{U})\boldsymbol{\rho}(\mathbf{W}|\mathbf{U})^\top\right] = E\left[\boldsymbol{\rho}(\mathbf{W}|\mathbf{U})\boldsymbol{\rho}(\mathbf{X}|\mathbf{U})^\top\right] = E\left[\boldsymbol{\rho}(\mathbf{W}|\mathbf{U})\boldsymbol{\rho}(\mathbf{Y}|\mathbf{U})^\top\right] = \mathbf{J}(\mathbf{W}|\mathbf{U}) \tag{397}$$

Thus, using (387)-(389), (392), (396)-(397) in (386), we get

$$\mathbf{0} \preceq \mathbf{A}\mathbf{J}(\mathbf{X}|\mathbf{U})\mathbf{A}^\top - \mathbf{A}\mathbf{J}(\mathbf{W}|\mathbf{U}) + (\mathbf{I}-\mathbf{A})\mathbf{J}(\mathbf{Y}|\mathbf{U})(\mathbf{I}-\mathbf{A})^\top - (\mathbf{I}-\mathbf{A})\mathbf{J}(\mathbf{W}|\mathbf{U}) \tag{398}$$

$$- \mathbf{J}(\mathbf{W}|\mathbf{U})\mathbf{A}^\top - \mathbf{J}(\mathbf{W}|\mathbf{U})(\mathbf{I}-\mathbf{A})^\top + \mathbf{J}(\mathbf{W}|\mathbf{U}) \tag{399}$$

$$= \mathbf{A}\mathbf{J}(\mathbf{X}|\mathbf{U})\mathbf{A}^\top + (\mathbf{I}-\mathbf{A})\mathbf{J}(\mathbf{Y}|\mathbf{U})(\mathbf{I}-\mathbf{A})^\top - \mathbf{J}(\mathbf{W}|\mathbf{U}) \tag{400}$$

which completes the proof.

# E Proof of Lemma 17

Consider $\mathbf{J}(\mathbf{X}|\mathbf{U})$

$$\mathbf{J}(\mathbf{X}|\mathbf{U}) = \mathbf{J}(\mathbf{X}|\mathbf{U},\mathbf{V}) \tag{401}$$

$$= E\left[\nabla_{\mathbf{x}}\log f(\mathbf{X}|\mathbf{U},\mathbf{V})\nabla_{\mathbf{x}}\log f(\mathbf{X}|\mathbf{U},\mathbf{V})^\top\right] \tag{402}$$

$$= E\left[\nabla_{\mathbf{x}}\log f(\mathbf{X},\mathbf{U},\mathbf{V})\nabla_{\mathbf{x}}\log f(\mathbf{X},\mathbf{U},\mathbf{V})^\top\right] \tag{403}$$

$$= E\Big[\big(\nabla_{\mathbf{x}}\log f(\mathbf{X},\mathbf{V}) + \nabla_{\mathbf{x}}\log f(\mathbf{U}|\mathbf{X},\mathbf{V})\big) \big(\nabla_{\mathbf{x}}\log f(\mathbf{X},\mathbf{V}) + \nabla_{\mathbf{x}}\log f(\mathbf{U}|\mathbf{X},\mathbf{V})\big)^\top\Big] \tag{404}$$

$$\begin{aligned} &= E\left[\nabla_{\mathbf{x}}\log f(\mathbf{X},\mathbf{V})\nabla_{\mathbf{x}}\log f(\mathbf{X},\mathbf{V})^\top\right] \\ &\quad + E\left[\nabla_{\mathbf{x}}\log f(\mathbf{X},\mathbf{V})\nabla_{\mathbf{x}}\log f(\mathbf{U}|\mathbf{X},\mathbf{V})^\top\right] \\ &\quad + E\left[\nabla_{\mathbf{x}}\log f(\mathbf{U}|\mathbf{X},\mathbf{V})\nabla_{\mathbf{x}}\log f(\mathbf{X},\mathbf{V})^\top\right] \\ &\quad + E\left[\nabla_{\mathbf{x}}\log f(\mathbf{U}|\mathbf{X},\mathbf{V})\nabla_{\mathbf{x}}\log f(\mathbf{U}|\mathbf{X},\mathbf{V})^\top\right] \end{aligned} \tag{405}$$

where (401) is due to the Markov chain $\mathbf{V} \to \mathbf{U} \to \mathbf{X}$, (403) comes from the fact that

$$\nabla_{\mathbf{x}}\log f(\mathbf{x}|\mathbf{u},\mathbf{v}) = \nabla_{\mathbf{x}}\big(\log f(\mathbf{x},\mathbf{u},\mathbf{v}) - \log f(\mathbf{u},\mathbf{v})\big) \tag{406}$$

$$= \nabla_{\mathbf{x}}\log f(\mathbf{x},\mathbf{u},\mathbf{v}) \tag{407}$$

and (404) is due to the fact that $f(\mathbf{x},\mathbf{u},\mathbf{v}) = f(\mathbf{x},\mathbf{v})f(\mathbf{u}|\mathbf{x},\mathbf{v})$. We note that

$$\mathbf{J}(\mathbf{X}|\mathbf{V}) = E\left[\nabla_{\mathbf{x}} \log f(\mathbf{X},\mathbf{V}) \nabla_{\mathbf{x}} \log f(\mathbf{X},\mathbf{V})^{\top}\right] \tag{408}$$

and

$$E\left[\nabla_{\mathbf{x}} \log f(\mathbf{U}|\mathbf{X},\mathbf{V}) \nabla_{\mathbf{x}} \log f(\mathbf{U}|\mathbf{X},\mathbf{V})^{\top}\right] \succeq \mathbf{0} \tag{409}$$

Using (408) and (409) in (405), we get

$$\begin{aligned}\mathbf{J}(\mathbf{X}|\mathbf{U}) \succeq \mathbf{J}(\mathbf{X}|\mathbf{V}) &+ E\left[\nabla_{\mathbf{x}} \log f(\mathbf{X},\mathbf{V}) \nabla_{\mathbf{x}} \log f(\mathbf{U}|\mathbf{X},\mathbf{V})^{\top}\right] \\ &+ E\left[\nabla_{\mathbf{x}} \log f(\mathbf{U}|\mathbf{X},\mathbf{V}) \nabla_{\mathbf{x}} \log f(\mathbf{X},\mathbf{V})^{\top}\right] \end{aligned} \tag{410}$$

We now show that the cross-terms in (410) vanish. To this end, consider the $(i,j)$th entry of the first cross-term

$$\begin{aligned} E\Big[\nabla_{\mathbf{x}} \log f(\mathbf{X},\mathbf{V}) \nabla_{\mathbf{x}} \log f(\mathbf{U}|\mathbf{X},\mathbf{V})^{\top}\Big]_{ij} &= E\left[\frac{\partial \log f(\mathbf{X},\mathbf{V})}{\partial x_i}\frac{\partial \log f(\mathbf{U}|\mathbf{X},\mathbf{V})}{\partial x_j}\right] && (411)\\ &= \int \frac{\frac{\partial f(\mathbf{x},\mathbf{v})}{\partial x_i}}{f(\mathbf{x},\mathbf{v})}\frac{\frac{\partial f(\mathbf{u}|\mathbf{x},\mathbf{v})}{\partial x_j}}{f(\mathbf{u}|\mathbf{x},\mathbf{v})} \; f(\mathbf{x},\mathbf{u},\mathbf{v}) \; d\mathbf{u} \; d\mathbf{v} \; d\mathbf{x} && (412)\\ &= \int \frac{\partial f(\mathbf{x},\mathbf{v})}{\partial x_i}\frac{\partial f(\mathbf{u}|\mathbf{x},\mathbf{v})}{\partial x_j} \; d\mathbf{u} \; d\mathbf{v} \; d\mathbf{x} && (413)\\ &= \int \frac{\partial f(\mathbf{x},\mathbf{v})}{\partial x_i}\left[\int \frac{\partial f(\mathbf{u}|\mathbf{x},\mathbf{v})}{\partial x_j} \; d\mathbf{u}\right] \; d\mathbf{v} \; d\mathbf{x} && (414)\end{aligned}$$

where the inner integral can be evaluated as

$$\int \frac{\partial f(\mathbf{u}|\mathbf{x},\mathbf{v})}{\partial x_j} \; d\mathbf{u} = \frac{\partial}{\partial x_j}\left[\int f(\mathbf{u}|\mathbf{x},\mathbf{v}) \; d\mathbf{u}\right] = \frac{\partial (1)}{\partial x_j} = 0 \tag{415}$$

where the interchange of the differentiation and the integration is justified by the assumption given in (206). Thus, using (415) in (414) implies that

$$E\Big[\nabla_{\mathbf{x}} \log f(\mathbf{X},\mathbf{V}) \nabla_{\mathbf{x}} \log f(\mathbf{U}|\mathbf{X},\mathbf{V})^{\top}\Big] = \mathbf{0} \tag{416}$$

Thus, using (416) in (410), we get

$$\mathbf{J}(\mathbf{X}|\mathbf{U}) \succeq \mathbf{J}(\mathbf{X}|\mathbf{V}) \tag{417}$$

which completes the proof.

# F Proof of Lemma 18

Since we assumed $\mu_j > 0,\ j = 1, \dots, m$, we can select

$$\tilde{\mathbf{\Sigma}}_{j+1} = \left[ \left( \sum_{i=1}^{j} \mathbf{K}_i + \mathbf{\Sigma}_{j+1} \right)^{-1} + \frac{1}{\mu_{j+1}} \mathbf{M}_{j+1} \right]^{-1} - \sum_{i=1}^{j} \mathbf{K}_i, \quad j = 0, 1 \dots, m-1 \tag{418}$$

which is equivalent to

$$\mu_{j+1} \left( \sum_{i=1}^{j} \mathbf{K}_i + \tilde{\mathbf{\Sigma}}_{j+1} \right)^{-1} = \mu_{j+1} \left( \sum_{i=1}^{j} \mathbf{K}_i + \mathbf{\Sigma}_{j+1} \right)^{-1} + \mathbf{M}_{j+1}, \quad j = 0, 1 \dots, m-1 \tag{419}$$

and that implies $\mathbf{0} \preceq \tilde{\mathbf{\Sigma}}_j \preceq \mathbf{\Sigma}_j,\ j=1,\ldots,m$. Furthermore, for $j=0,\ldots,m-1$, we have

$$\sum_{i=1}^{j+1}\mathbf{K}_i + \tilde{\mathbf{\Sigma}}_{j+1} = \mathbf{K}_{j+1} + \left(\sum_{i=1}^{j}\mathbf{K}_i + \tilde{\mathbf{\Sigma}}_{j+1}\right) \tag{420}$$

$$= \mathbf{K}_{j+1} + \left[\left(\sum_{i=1}^{j}\mathbf{K}_i + \mathbf{\Sigma}_{j+1}\right)^{-1} + \frac{1}{\mu_{j+1}}\mathbf{M}_{j+1}\right]^{-1} \tag{421}$$

$$= \mathbf{K}_{j+1} + \left[\mathbf{I} + \frac{1}{\mu_{j+1}}\left(\sum_{i=1}^{j}\mathbf{K}_i + \mathbf{\Sigma}_{j+1}\right)\mathbf{M}_{j+1}\right]^{-1}\left(\sum_{i=1}^{j}\mathbf{K}_i + \mathbf{\Sigma}_{j+1}\right) \tag{422}$$

$$= \mathbf{K}_{j+1} + \left[\mathbf{I} + \frac{1}{\mu_{j+1}}\left(\sum_{i=1}^{j+1}\mathbf{K}_i + \mathbf{\Sigma}_{j+1}\right)\mathbf{M}_{j+1}\right]^{-1}\left(\sum_{i=1}^{j}\mathbf{K}_i + \mathbf{\Sigma}_{j+1}\right) \tag{423}$$

$$= \mathbf{K}_{j+1} + \left[\left(\sum_{i=1}^{j+1}\mathbf{K}_i + \mathbf{\Sigma}_{j+1}\right)^{-1} + \frac{1}{\mu_{j+1}}\mathbf{M}_{j+1}\right]^{-1}\left(\sum_{i=1}^{j+1}\mathbf{K}_i + \mathbf{\Sigma}_{j+1}\right)^{-1}\left(\sum_{i=1}^{j}\mathbf{K}_i + \mathbf{\Sigma}_{j+1}\right) \tag{424}$$

$$= \mathbf{K}_{j+1} + \left[\left(\sum_{i=1}^{j+1}\mathbf{K}_i + \mathbf{\Sigma}_{j+1}\right)^{-1} + \frac{1}{\mu_{j+1}}\mathbf{M}_{j+1}\right]^{-1}\left(\sum_{i=1}^{j+1}\mathbf{K}_i + \mathbf{\Sigma}_{j+1}\right)^{-1} \times \left(\sum_{i=1}^{j+1}\mathbf{K}_i + \mathbf{\Sigma}_{j+1} - \mathbf{K}_{j+1}\right) \tag{425}$$

$$= \mathbf{K}_{j+1} + \left[\left(\sum_{i=1}^{j+1}\mathbf{K}_i + \mathbf{\Sigma}_{j+1}\right)^{-1} + \frac{1}{\mu_{j+1}}\mathbf{M}_{j+1}\right]^{-1} - \left[\left(\sum_{i=1}^{j+1}\mathbf{K}_i + \mathbf{\Sigma}_{j+1}\right)^{-1} + \frac{1}{\mu_{j+1}}\mathbf{M}_{j+1}\right]^{-1}\left(\sum_{i=1}^{j+1}\mathbf{K}_i + \mathbf{\Sigma}_{j+1}\right)^{-1}\mathbf{K}_{j+1} \tag{426}$$

$$= \mathbf{K}_{j+1} + \left[\left(\sum_{i=1}^{j+1}\mathbf{K}_i + \mathbf{\Sigma}_{j+1}\right)^{-1} + \frac{1}{\mu_{j+1}}\mathbf{M}_{j+1}\right]^{-1} - \left[\left(\sum_{i=1}^{j+1}\mathbf{K}_i + \mathbf{\Sigma}_{j+1}\right)^{-1} + \frac{1}{\mu_{j+1}}\mathbf{M}_{j+1}\right]^{-1}\left[\left(\sum_{i=1}^{j+1}\mathbf{K}_i + \mathbf{\Sigma}_{j+1}\right)^{-1} + \frac{1}{\mu_{j+1}}\mathbf{M}_{j+1}\right]\mathbf{K}_{j+1} \tag{427}$$

$$= \mathbf{K}_{j+1} + \left[\left(\sum_{i=1}^{j+1}\mathbf{K}_i + \mathbf{\Sigma}_{j+1}\right)^{-1} + \frac{1}{\mu_{j+1}}\mathbf{M}_{j+1}\right]^{-1} - \mathbf{K}_{j+1} \tag{428}$$

$$= \left[\left(\sum_{i=1}^{j+1}\mathbf{K}_i + \mathbf{\Sigma}_{j+1}\right)^{-1} + \frac{1}{\mu_{j+1}}\mathbf{M}_{j+1}\right]^{-1} \tag{429}$$

where (421) follows from (419), (423) and (427) are consequences of the KKT conditions $\mathbf{M}_j\mathbf{K}_j = \mathbf{K}_j\mathbf{M}_j = \mathbf{0},\ j = 1, \ldots, m$. Finally, (429) is equivalent to

$$\mu_{j+1}\left(\sum_{i=1}^{j+1}\mathbf{K}_i + \tilde{\mathbf{\Sigma}}_{j+1}\right)^{-1} = \mu_{j+1}\left(\sum_{i=1}^{j+1}\mathbf{K}_i + \mathbf{\Sigma}_{j+1}\right)^{-1} + \mathbf{M}_{j+1}, \quad j = 0, \ldots, m-1 \tag{430}$$

Plugging (419) and (430) into the KKT conditions in (288) and (289) yields the third part of the lemma.

We now prove the second part of the lemma. To this end, consider the second equation of the third part of the lemma, i.e., the following

$$\mu_m\left(\sum_{i=1}^{m}\mathbf{K}_i + \tilde{\mathbf{\Sigma}}_m\right)^{-1} = \mu_m\left(\sum_{i=1}^{m}\mathbf{K}_i + \mathbf{\Sigma}_Z\right)^{-1} + \mathbf{M}_Z \tag{431}$$

which implies $\tilde{\mathbf{\Sigma}}_m \preceq \mathbf{\Sigma}_Z$. Now, consider the first equation of the third part of the lemma for $j = m-1$, i.e., the following

$$\begin{aligned}\mu_{m-1}\left(\sum_{i=1}^{m-1}\mathbf{K}_i + \tilde{\mathbf{\Sigma}}_{m-1}\right)^{-1} - \mu_{m-1}\left(\sum_{i=1}^{m-1}\mathbf{K}_i + \mathbf{\Sigma}_Z\right)^{-1} &= \mu_m\left(\sum_{i=1}^{m-1}\mathbf{K}_i + \tilde{\mathbf{\Sigma}}_m\right)^{-1} \\ &\quad - \mu_m\left(\sum_{i=1}^{m-1}\mathbf{K}_i + \mathbf{\Sigma}_Z\right)^{-1}\end{aligned} \tag{432}$$

Since the matrix on the right hand side of the equation is positive semi-definite due to the fact that $\tilde{\mathbf{\Sigma}}_m \preceq \mathbf{\Sigma}_Z$, and we assume that $\mu_m \geq \mu_{m-1}$, (432) implies

$$\left(\sum_{i=1}^{m-1}\mathbf{K}_i + \tilde{\mathbf{\Sigma}}_{m-1}\right)^{-1} - \left(\sum_{i=1}^{m-1}\mathbf{K}_i + \mathbf{\Sigma}_Z\right)^{-1} \succeq \left(\sum_{i=1}^{m-1}\mathbf{K}_i + \tilde{\mathbf{\Sigma}}_m\right)^{-1} - \left(\sum_{i=1}^{m-1}\mathbf{K}_i + \mathbf{\Sigma}_Z\right)^{-1} \tag{433}$$

which in turn implies $\tilde{\mathbf{\Sigma}}_{m-1} \preceq \tilde{\mathbf{\Sigma}}_m \preceq \mathbf{\Sigma}_Z$. Similarly, if one keeps checking the first equation of the third part of the lemma in the reverse order, one can get

$$\tilde{\mathbf{\Sigma}}_1 \preceq \ldots \preceq \tilde{\mathbf{\Sigma}}_m \preceq \mathbf{\Sigma}_Z \tag{434}$$

Moreover, the definition of $\tilde{\mathbf{\Sigma}}_1$, i.e., (419) for $j = 0$,

$$\tilde{\mathbf{\Sigma}}_1 = \left[\mathbf{\Sigma}_1^{-1} + \frac{1}{\mu_1}\mathbf{M}_1\right]^{-1} \tag{435}$$

implies that $\tilde{\mathbf{\Sigma}}_1 \succ \mathbf{0}$ completing the proof of the second part of the lemma.

We now show the fourth part of the lemma

$$\begin{aligned}
&\left(\sum_{i=1}^{j+1}\mathbf{K}_i+\tilde{\mathbf{\Sigma}}_{j+1}\right)^{-1}\left(\sum_{i=1}^{j}\mathbf{K}_i+\tilde{\mathbf{\Sigma}}_{j+1}\right)\\
&\qquad=\left(\sum_{i=1}^{j+1}\mathbf{K}_i+\tilde{\mathbf{\Sigma}}_{j+1}\right)^{-1}\left(\sum_{i=1}^{j+1}\mathbf{K}_i+\tilde{\mathbf{\Sigma}}_{j+1}-\mathbf{K}_{j+1}\right) && (436)\\
&\qquad=\mathbf{I}-\left(\sum_{i=1}^{j+1}\mathbf{K}_i+\tilde{\mathbf{\Sigma}}_{j+1}\right)^{-1}\mathbf{K}_{j+1} && (437)\\
&\qquad=\mathbf{I}-\left[\left(\sum_{i=1}^{j+1}\mathbf{K}_i+\mathbf{\Sigma}_{j+1}\right)^{-1}+\frac{1}{\mu_{j+1}}\mathbf{M}_{j+1}\right]\mathbf{K}_{j+1} && (438)\\
&\qquad=\mathbf{I}-\left(\sum_{i=1}^{j+1}\mathbf{K}_i+\mathbf{\Sigma}_{j+1}\right)^{-1}\mathbf{K}_{j+1} && (439)\\
&\qquad=\left(\sum_{i=1}^{j+1}\mathbf{K}_i+\mathbf{\Sigma}_{j+1}\right)^{-1}\left(\sum_{i=1}^{j+1}\mathbf{K}_i+\mathbf{\Sigma}_{j+1}\right)-\left(\sum_{i=1}^{j+1}\mathbf{K}_i+\mathbf{\Sigma}_{j+1}\right)^{-1}\mathbf{K}_{j+1} && (440)\\
&\qquad=\left(\sum_{i=1}^{j+1}\mathbf{K}_i+\mathbf{\Sigma}_{j+1}\right)^{-1}\left(\sum_{i=1}^{j}\mathbf{K}_i+\mathbf{\Sigma}_{j+1}\right),\quad j=0,\ldots,m-1 && (441)
\end{aligned}$$

where (438) follows from (430) and (439) is a consequence of the KKT conditions $\mathbf{K}_j\mathbf{M}_j=\mathbf{M}_j\mathbf{K}_j=\mathbf{0},\ j=1,\ldots,m$.

The proof of the fifth part of the lemma follows similarly

$$
\begin{aligned}
\left(\mathbf{S}+\tilde{\mathbf{\Sigma}}_m\right)\left(\sum_{i=1}^m \mathbf{K}_i+\tilde{\mathbf{\Sigma}}_m\right)^{-1} &= \left(\mathbf{S}-\sum_{i=1}^m \mathbf{K}_i+\sum_{i=1}^m \mathbf{K}_i+\tilde{\mathbf{\Sigma}}_m\right)\left(\sum_{i=1}^m \mathbf{K}_i+\tilde{\mathbf{\Sigma}}_m\right)^{-1} \\
&= \left(\mathbf{S}-\sum_{i=1}^m \mathbf{K}_i\right)\left(\sum_{i=1}^m \mathbf{K}_i+\tilde{\mathbf{\Sigma}}_m\right)^{-1}+\mathbf{I} \qquad (442) \\
&= \left(\mathbf{S}-\sum_{i=1}^m \mathbf{K}_i\right)\left[\left(\sum_{i=1}^m \mathbf{K}_i+\mathbf{\Sigma}_Z\right)^{-1}+\frac{1}{\mu_m}\mathbf{M}_Z\right]+\mathbf{I} \qquad (443) \\
&= \left(\mathbf{S}-\sum_{i=1}^m \mathbf{K}_i\right)\left(\sum_{i=1}^m \mathbf{K}_i+\mathbf{\Sigma}_Z\right)^{-1}+\mathbf{I} \qquad (444) \\
&= \left(\mathbf{S}-\sum_{i=1}^m \mathbf{K}_i\right)\left(\sum_{i=1}^m \mathbf{K}_i+\mathbf{\Sigma}_Z\right)^{-1}+ \\
&\quad \left(\sum_{i=1}^m \mathbf{K}_i+\mathbf{\Sigma}_Z\right)\left(\sum_{i=1}^m \mathbf{K}_i+\mathbf{\Sigma}_Z\right)^{-1} \qquad (445) \\
&= (\mathbf{S}+\mathbf{\Sigma}_Z)\left(\sum_{i=1}^m \mathbf{K}_i+\mathbf{\Sigma}_Z\right)^{-1} \qquad (446)
\end{aligned}
$$

where (443) follows from the second equation of the third part of the lemma, and (444) is a consequence of the KKT condition in (285), completing the proof.

# References


[1] A. Wyner. The wire-tap channel. *Bell System Technical Journal*, 54(8):1355–1387, Jan. 1975.

[2] I. Csiszar and J. Korner. Broadcast channels with confidential messages. *IEEE Trans. Inf. Theory*, IT-24(3):339–348, May 1978.

[3] E. Tekin and A. Yener. The Gaussian multiple access wire-tap channel. *IEEE Trans. Inf. Theory*, 54(12):5747–5755, Dec. 2008.

[4] E. Tekin and A. Yener. The general Gaussian multiple access and two-way wire-tap channels: Achievable rates and cooperative jamming. *IEEE Trans. Inf. Theory*, 54(6):2735–2751, Jun. 2008.

[5] E. Ekrem and S. Ulukus. On the secrecy of multiple access wiretap channel. In *46th Annual Allerton Conference on Communications, Control and Computing*, Sep. 2008.

[6] R. Liu, I. Maric, P. Spasojevic, and R. D. Yates. Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions. *IEEE Trans. Inf. Theory*, 54(6):2493–2507, Jun. 2008.

[7] R. Liu and H. V. Poor. Secrecy capacity region of a multi-antenna Gaussian broadcast channel with confidential messages. *IEEE Trans. Inf. Theory*, 55(3):1235–1249, Mar. 2009.

[8] A. Khisti, A. Tchamkerten, and G. W. Wornell. Secure broadcasting over fading channels. *IEEE Trans. Inf. Theory*, 54(6):2453–2469, Jun. 2008.

[9] G. Bagherikaram, A. S. Motahari, and A. K. Khandani. The secrecy rate region of the broadcast channel. In *46th Annual Allerton Conf. Commun., Contr. and Comput.*, Sep. 2008. Also available at [arXiv:0806.4200].

[10] E. Ekrem and S. Ulukus. On secure broadcasting. In *42th Asilomar Conf. Signals, Syst. and Comp.*, Oct. 2008.

[11] E. Ekrem and S. Ulukus. Secrecy capacity of a class of broadcast channels with an eavesdropper. Submitted to *EURASIP Journal on Wireless Communications and Networking*, Dec. 2008. Also available at [arXiv:0812.0319].

[12] Y. Oohama. Relay channels with confidential messages. Submitted to *IEEE Trans. Inf. Theory,* Mar. 2007. Also available at [arXiv:0611125].

[13] L. Lai and H. El Gamal. The relay-eavesdropper channel: Cooperation for secrecy. *IEEE Trans. Inf. Theory*, 54(9):4005–4019, Sep. 2008.

[14] M. Yuksel and E. Erkip. The relay channel with a wire-tapper. In *41st Annual Conf. on Inf. Sciences and Syst.*, Mar. 2007.

[15] X. He and A. Yener. Cooperation with an untrusted relay: A secrecy perspective. submitted to *IEEE Trans. Inf. Theory*, Oct. 2008.

[16] E. Ekrem and S. Ulukus. Effects of cooperation on the secrecy of multiple access channels with generalized feedback. In *Conference on Information Sciences and Systems*, Mar. 2008.

[17] E. Ekrem and S. Ulukus. Secrecy in cooperative relay broadcast channels. Submitted to *IEEE Trans. Inf. Theory*, Oct. 2008. Also available at [arXiv:0811.1317].

[18] M. Bloch and A. Thangaraj. Confidential messages to a cooperative relay. In *IEEE Information Theory Workshop*, May 2008.

[19] Y. Liang and H. V. Poor. Multiple access channels with confidential messages. *IEEE Trans. Inf. Theory*, 54(3):976–1002, Mar. 2008.

[20] R. Liu, I. Maric, R. D. Yates, and P. Spasojevic. The discrete memoryless multiple access channel with confidential messages. In *IEEE Int. Symp. Inf. Theory*, Jul. 2006.

[21] X. Tang, R. Liu, P. Spasojevic, and H. V. Poor. Multiple access channels with generalized feedback and confidential messages. In *IEEE Inf. Theory Workshop on Frontiers in Coding Theory*, Sep. 2007.

[22] P. Bergmans. A simple converse for broadcast channels with additive white Gaussian noise. *IEEE Trans. Inf. Theory*, 20(3):279–280, Mar. 1974.

[23] A. El Gamal. EE478 Multiple user information theory. Lecture notes.

[24] A. J. Stam. Some inequalities satisfied by the quantities of information of Fisher and Shannon. *Information and Control*, 2:101–112, Jun. 1959.

[25] N. M. Blachman. The convolution inequality for entropy powers. *IEEE Trans. Inf. Theory*, IT-11(2):267–271, Apr. 1965.

[26] D. Guo, S. Shamai (Shitz), and S. Verdu. Mutual information and minimum mean-square error in Gaussian channels. *IEEE Trans. Inf. Theory*, 51(4):1261–1283, Apr. 2005.

[27] D. Guo, S. Shamai (Shitz), and S. Verdu. Estimation of non-Gaussian random variables in Gaussian noise: Properties of the MMSE. In *IEEE ISIT*, Jul. 2008. Also submitted to *IEEE Trans. Inf. Theory.*

[28] O. Rioul. Information theoretic proofs of entropy power inequalities. Submitted to *IEEE Trans. Inf. Theory,* Apr. 2007. Also available at [arXiv:0704.1751].

[29] H. Weingarten, Y. Steinberg, and S. Shamai (Shitz). The capacity region of the Gaussian multiple-input multiple-output broadcast channel. *IEEE Trans. Inf. Theory*, 52(9):3936–3964, Sep. 2006.

[30] T. Liu and S. Shamai (Shitz). A note on the secrecy capacity of the multi-antenna wiretap channel. Submitted to *IEEE Trans. Inf. Theory*, Dec. 2007. Also available at http://www.ece.tamu.edu/∼tieliu/publications.html.

[31] D. P. Palomar and S. Verdu. Gradient of mutual information in linear vector Gaussian channels. *IEEE Trans. Inf. Theory*, 52(1):141–154, Jan. 2006.

[32] A. Khisti and G. Wornell. Secure transmission with multiple antennas II: The MIMOME channel. Submitted to *IEEE Trans. Inf. Theory*, Aug. 2008. Also available at http://allegro.mit.edu/bin/pubs-search.php.

[33] F. Oggier and B. Hassibi. The secrecy capacity of the MIMO wiretap channel. Submitted to *IEEE Trans. Inf. Theory*, Oct. 2007. Also available at [arXiv:0710.1920].

[34] S. Shafiee, N. Liu, and S. Ulukus. Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel. *IEEE Trans. Inf. Theory*, Sep. 2007. To appear. Also available at [arXiv:0709.3541].

[35] S. K. Leung-Yan-Cheong and M. E. Hellman. The Gaussian wire-tap channel. *IEEE Trans. Inf. Theory*, 24(4):451–456, Jul. 1978.

[36] O. Johnson. *Information theory and the central limit theorem.* Imperial College Press, 2004.

[37] S. Ihara. On the capacity of channels with additive non-Gaussian noise. *Information and Control*, 37(1):34–39, Apr. 1978.

[38] S. H. Diggavi and T. M. Cover. The worst additive noise constraint under a covariance constraint. *IEEE Trans. Inf. Theory*, 47(7):3072–3081, Nov. 2001.

[39] T. Liu and P. Viswanath. An extremal inequality motivated by multiterminal information theoretic problems. *IEEE Trans. Inf. Theory*, 53(5):1839–1851, May 2007.

[40] R. A. Horn and C. R. Johnson. *Matrix Analysis.* Cambridge, 1985.

[41] K. Marton. A coding theorem for the discrete memoryless channels. *IEEE Trans. Inf. Theory*, 25(1):306–311, May 1979.

[42] W. Yu and J. Cioffi. Sum capacity of Gaussian vector broadcast channels. *IEEE Trans. Inf. Theory*, 50(9):1875–1892, Sep. 2004.